POLYNOMIAL METHODS: RECENT ADVANCEMENTS IN COMBINATORICS

by

Thomas Fleming

A Thesis

Submitted in Partial Fulfillment of the

Requirements for the Degree of

Master of Science

Major: Mathematical Sciences

The University of Memphis

May 2022

ACKNOWLEDGMENTS

First and foremost, I would like to thank my advisor and professor, Dr. Grynkiewicz. He supplied me with many of the ideas for this thesis, clarified seemingly mystical results, and helped me through many rounds of revisions. I would also like to thank the attending professors for my Thesis defense, Dr. Wierdl and Dr. Nikiforov, who were kind enough to supervise my defense only days before spring break. Finally, I would like to thank my family and my fiancee, Amber.

ABSTRACT

Fleming, Thomas Rexford. M.Sc. The University of Memphis. May 2022. Polynomial Methods: Recent Advancements in Combinatorics. Major Professor: Dr. David Grynkiewicz.

In this Master's Thesis, we showcase the use of an array of results collectively known as the polynomial method. First, we lay groundwork, giving some basic definitions, notation, and prerequisites. Then, we introduce three related theorems, the Combinatorial Nullstellensatz, Generalized Combinatorial Nullstellensatz, and Punctured Combinatorial Nullstellensatz, each concerning properties of multivariate polynomials with specific constraints on their degree. With these results proven, we then showcase some simple combinatorial and graph theoretic results which have very simple proofs making use of the Nullstellensatz theorems. In chapter 4 we give the proof of the q-Dyson theorem as published by Zeilberger and Bressoud. Finally, in chapters $5, 6$ and 7 we introduce zero-sum theory, prove the Davenport constant of finite abelian p-groups without making use of group rings, and then state and prove the Chevalley-Warning theorem and use it to prove the Kemnitz conjecture on zero-sums in cyclic groups.

TABLE OF CONTENTS

Chapter 1

Introduction and Preliminary Results

Introduction

One of the earliest objects of algebraic study, real (specifically integral) univariate polynomials generalize the most simple algebraic objects, linear functions, and have many significant applications. Multivariate polynomials offer further generalization. Expanding even further, multivariate polynomials over arbitrary rings (and fields) prove surprisingly useful. In this thesis, we will showcase a variety of methods and applications involving polynomials. These applications will prove some surprising results, both abstract and concrete. To understand these proofs, one need only basic knowledge of algebraic tools and structures, and some experience with methods of combinatorial proof.

Merging the fields of Combinatorics and Number Theory yields Combinatorial Number Theory and Additive Combinatorics, two overlapping fields answering questions pertaining to zero-sums over sequences and zeroes of arbitrary polynomials, as well as other problems at the intersection of Combinatorics, Algebra, and Number Theory. We begin Chapter 1 by presenting many common objects which we will make use of throughout the thesis. This will include some objects of common study, such as polynomials, as well as some notation and conventions common to the field, and the statements of a few common theorems which the reader will likely be familiar with. After this, in chapter 2, we introduce the Nullstellensatz theorems, literally translating as zero-locus theorem, which characterize a polynomial based on its number of zeroes. These theorems, while extremely powerful, will have relatively simple statements and proofs culminating in the Punctured Nullstellensatz. Moving on, in chapter 3 we demonstrate some applications of these Nullstellensatz theorems. These will mostly make use of the simplest version of the Nullstellensatz which we present, Alon's Combinatorial Nullstellensatz II [1]. The applications will come in two main varieties, sumset proofs and

graph theoretic proofs. This chapter will provide some of the most concrete applications of the polynomial method. In chapter 4 we present Dyson's Theorem [9] on laurent polynomials and Zeilberger and Bressoud's q-Dyson variant [8], with a proof based on a concrete version of the Combinatorial Nullstellensatz. In chapter 5 we provide a short introduction to zero-sum theory along with a few basic results. Then, in chapter 6, we prove the davenport constant D of finite abelian p-groups. This proof, though similar to one used by Christian Elsholtz in [5], is hitherto unpublished. Finally, in chapter 7, we prove the Kemnitz conjecture concerning zero-sum sequences in C_n^2. First, though, we must state some prerequisites which we will make use of throughout this thesis.

Definitions, Notation, and Preliminary Results

Before we continue on, we define a few basic objects which we will make regular use of and 3 algebraic results which will go unproven throughout the thesis. Readers are assumed to have knowledge equivalent to a first course in group and ring theory and a first course in combinatorics.

Definition 1.1 (Polynomial Ring)**.** Given a commutative ring R, we define $R[x]$ to be the ring generated by all formal sums of the form $f = \sum_{i=0}^{\infty} c_i x^i$, $c_i \in R$ where $c_i \neq 0$ for only finitely many $i \in \mathbb{N}_0$. Given $f = \sum_{i=0}^{\infty} a_i x^i$, $g = \sum_{i=0}^{\infty} b_i x^i$ we define $f + g = \sum_{i=0}^{\infty} (a_i + b_i) x^i$ and $fg = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} a_i b_j x^{i+j}$. It is routinely checked that these operations, together with the set of all such polynomials $f \in R[x]$, form a ring. We call $R[x]$ equipped with $+$ and $\cdot$ **the polynomial ring** in 1 variable over R. We call a polynomial monic if the coefficient of its highest power term is 1.

Definition 1.2 (Multivariate Polynomial Ring)**.** Given a ring R, we define a **polynomial ring** over n variables, $R[x_1, \ldots, x_n]$ inductively by the rules $R[x_1] = R[x]$ and $R[x_1, \ldots, x_i] = (R[x_1, \ldots, x_{i-1}])[x_i]$.

Definition 1.3 (Laurent Polynomial Ring)**.** Given a field F, we define a **univariate laurent polynomial** to be a formal sum of the form: $f = \sum_{i=-\infty}^{\infty} a_i x^i$ with $a_i \in F$ and $a_i \neq 0$ for only finitely many $i \in \mathbb{Z}$. Multiplication and addition are defined just as with standard polynomial rings, except with the added relation $x \cdot x^{-1} = 1$.

We define a **multivariate laurent polynomial** over n variables to be a formal sum of the form: $f = \sum_{i_1,\ldots,i_n \in \mathbb{Z}} c_{i_1,\ldots,i_n} x_1^{i_1} \ldots x_n^{i_n}$ with $c_{i_1,\ldots,i_n} \neq 0$ for only finitely many tuples

$(i_1, \ldots, i_n) \in \mathbb{Z}^n$.

Once again, it is routinely checked that the set of all laurent polynomials in n-variables with coefficients in F, together with $+$ and $\cdot$ and the relation $x_i \cdot x_i^{-1} = 1$ $1 \leq i \leq n$, forms a ring for each $n \in \mathbb{N}$.

Definition 1.4 (Degree)**.** We define the **degree** of a polynomial $f \in R[x]$ as

$$\deg(f) = \min\{N \in \mathbb{N}_0 : c_i = 0 \; \forall \; i > N\}.$$

For multivariate polynomial rings there are two natural generalizations of degree, total degree and projected degree. For a polynomial

$$f = \sum_{i_1,\ldots,i_n \in \mathbb{N}_0} c_{i_1,\ldots,i_n} x_1^{i_1} \ldots x_n^{i_n} \in R[x_1, \ldots, x_n]$$

we define the **total degree** as

$$\deg(f) = \min\{N \in \mathbb{N}_0 : c_{i_1,\ldots,i_n} = 0 \; \forall \; i_1, \ldots, i_n \in \mathbb{N}_0 \text{ so that } \sum_{j=1}^{n} i_j > N\}$$

and we define the **projected degree** in variable x_k as the degree of f when interpreted as a polynomial in the ring $(R[x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n])[x_k]$. Essentially, this is the degree in only the variable x_k and it is denoted by $\deg_{x_k}(f)$.

Example.

$$\deg\left(x^2\right) = \deg\left(x^2 + x + 1\right) = \deg\left(x_1x_2 + x_1^2 + x_2^2 + 1\right) = \deg_{x_1}\left(x_1^2x_2^3x_3^4\right) = 2$$

Definition 1.5 (Module)**.** Given a ring R, we define a (left) R**-module** M to be a set endowed with two operations, addition and multiplication, such that $+ : M \times M \to M$ and $\cdot : R \times M \to M$ with $+$ satisfying the axioms of an abelian group and $\cdot$ being associative, having an identity, and having both left and right distributive laws: $(rs)(x) = r(sx)$, $1x = x$, $((r+s)x = rx + sx$, $r(x+y) = rx + ry$ for $r, s \in R$ and $x, y \in M$). If R is a field, we instead call M a vector space.

In a vector space M, we call a set B a basis of M if it is linearly independent and spans M.

Definition 1.6 (Characteristic Function)**.** Given a vector $\mathbf{x}$, the **characteristic function** $\chi_{\mathbf{x}}$ has $\chi_{\mathbf{x}}(\mathbf{y}) = \begin{cases} 1, & \mathbf{x} = \mathbf{y} \\ 0, & \mathbf{x} \neq \mathbf{y} \end{cases}$

Notation (Common Symbols)**.** Throughout this thesis we will make use of the following symbols, $\mathbb{Z}$ for the integers, $\mathbb{N}$ for the positive integers (not including 0), $\mathbb{N}_0$ for the nonnegative integers including 0, and $\mathbb{Q}$ for the rationals. Since we do not introduce any proofs using $\mathbb{R}$, we will use $[a, b] = \{x \in \mathbb{Z} : a \leq x \leq b\}$. Furthermore, G will be a group, R a ring, and F a field.

Notation (Polynomial Coefficient)**.** For a laurent polynomial

$$f = \sum_{i_1,\ldots,i_n \in \mathbb{Z}} c_{i_1,\ldots,i_n} x_1^{i_1} \ldots x_n^{i_n}$$

over n variables, we denote the coefficient of a particular term by $\left[x_1^{i_1} \dots x_n^{i_n}\right] f \coloneqq c_{i_1,\dots,i_n}$ when it is more convenient.

Notation (Vector Polynomials)**.** For a (laurent) polynomial $f(x_1, \dots, x_n)$ evaluated at $x_1, \dots, x_n$, we implicitly denote $\mathbf{x} = (x_1, \dots, x_n)$ and $f(\mathbf{x}) = f(x_1, \dots, x_n)$ when it is unambiguous and convenient.

Notation (Congruence)**.** For a congruence statement $a \equiv b \,(\mod c)$ we sometimes shorten it to $a \equiv b$ when the modulus c is unambiguous.

Notation (Cyclic Groups)**.** For a given $n \in \mathbb{N}$, we denote the cyclic group of order n as C_n, i.e., $\mathbb{Z}/n\mathbb{Z} = C_n$. Since $\mathbb{Z}/n\mathbb{Z}$ is also a field for prime p, we use it in this context as well.

The next theorem has many equivalent statements as well as a few stronger (and weaker) ones. For the rest of this thesis, we will assume the Fundamental Theorem of Algebra refers to the following statement.

Theorem 1.1 (Fundamental Theorem of Algebra)**.** Given an integral domain R and $f \in R[x]$ with f nonzero, let $X = \{x \in R : f(x) = 0\}$. Then, $|X| \leq n$.

Next, we provide the binomial theorem, or binomial coefficient theorem.

Theorem 1.2. Let p be prime, $f \in C_p[x, y]$, $0 \leq a < b \leq p$, then $\left[x^a y^{b-a}\right](x + y)^b = \binom{b}{a}$. So, $(x + y)^b = \sum_{a=0}^{b} \binom{b}{a} x^a y^{b-a}$.

This theorem is easily extended from the integers to the finite field C_p, so we neglect to prove it.

The next two theorems are routinely checked and commonly proved in a first introduction to ring theory.

Theorem 1.3. Let R be a ring. If R is a unique factorization domain, then $R[x_1, \ldots, x_n]$ is a unique factorization domain for all $n \in \mathbb{N}$.

Theorem 1.4. Let R be an integral domain and F its quotient field. If $x(x_1), y(\mathbf{x}) \in R[x_1, \ldots, x_n]$ with $x(x_1)$ being monic and $x(x_1) \mid y(\mathbf{x})$ over F then, $x(x_1) \mid y(\mathbf{x})$ over R.

This last prerequisite is a direct consequence of the pigeonhole principle

Theorem 1.5. Let G be a finite abelian group and let $A, B \subseteq G$ be nonempty subsets. If $|A| + |B| \geq |G| + 2$, then all elements $x \in G$ have at least 2 representations of the form $a_1 + b_1 = a_2 + b_2 = x$ where $a_1, a_2 \in A$, $b_1, b_2 \in B$ and $a_1 \neq a_2, b_1 \neq b_2$.

Indeed, this theorem can be generalized to hold for r representations $a_i + b_i$, $1 \leq i \leq r$. A good proof is found in [7].

Chapter 2

Nullstellensatz

Hilbert's Nullstellensatz

Before we can approach the Combinatorial Nullstellensatz, or any other tools of the polynomial method, it is important to see a closely related theorem, Hilbert's Nullstellensatz. This theorem is more algebraic in nature, though its influence in the Combinatorial Nullstellensatz will be clear. One statement of this theorem is as follows,

Theorem 2.1 (Hilbert's Nullstellensatz)**.** Let F be an algebraically closed field and $f, g_1, \ldots, g_m \in F[x_1, \ldots, x_n]$. Let $V(g_1, \ldots, g_m) = \{\mathbf{x} \in F^n : g_i(\mathbf{x}) = 0, 1 \leq i \leq m\}$. If $f(\mathbf{v}) = 0$ for all $\mathbf{v} \in V(g_1, g_2, \ldots, g_m)$, then there is an integer k and polynomials $h_1, \ldots, h_m \in F[x_1, \ldots, x_m]$ such that $f^k = \sum_{i=1}^{n} h_i g_i$.

For a proof of this, see [13].

This theorem, though closely related to the Combinatorial Nullstellensatz, will see no use in this thesis, though their historical and mathematical relation are good to keep in mind. With this, we now introduce the main tool of this thesis, Alon's Combinatorial Nullstellensatz.

Alon's Combinatorial Nullstellensatz

Alon's theorem actually falls under a special case of Hilbert's Nullstellensatz, when $n = m$ and each g_i is univariate and of the form $\prod_{s \in S_i} (x_i - s)$. However, these extra conditions allow a stronger conclusion to be drawn, namely that f can split into polynomials of lesser collective degree than itself. Though this statement is non-rigorous, it is immediately clear that turning one polynomial into a sum of simpler polynomials can have useful corollaries. It is in fact one of these corollaries that we will make use of throughout much of this thesis. Before we can prove such a theorem, though, we need to state and prove the following lemma:

Lemma 2.1. [1] Let R be an integral domain. Let $n \geq 1$, $f(\mathbf{x}) \in R[x_1, x_2, \ldots, x_n]$, and $A_1, A_2, \ldots, A_n \subseteq R$ be finite and nonempty.

Suppose $\deg_{x_i} f < |A_i|$ for each $1 \leq i \leq n$ and $f(\mathbf{a}) = 0$ for all $\mathbf{a} \in \prod_{i=1}^{n} A_i$. Then f is the zero polynomial.

Proof. Let F be the quotient field of R. Clearly, any polynomial in R is a polynomial in F, and as $f = 0$ in F implies $f = 0$ in R, we need only consider the case $F = R$. We will proceed by induction on n. We already know the case $n = 1$ holds by the Fundamental Theorem of Algebra. Now, we prove the case n. First, let us define $f_i(x_1, x_2, \ldots, x_{n-1})$ to be the coefficient of x_n^i when considering f as a polynomial in the ring $(F[x_1, \ldots, x_{n-1}])[x_n]$. Then,

$$f(\mathbf{x}) = \sum_{i=0}^{\deg_{x_n} f} f_i(x_1, x_2, \ldots, x_{n-1}) x_n^i.$$

We see each $f_i \in F[x_1, x_2, \ldots, x_{n-1}]$ and $\deg_{x_j} f_i \leq \deg_{x_j} f < |A_i|$ for all $1 \leq j \leq n-1$ and $0 \leq i \leq \deg_{x_n} f$. Let $a_i \in A_i$ be an arbitrary element for each $0 \leq i \leq n-1$. As $f(a_1, a_2, \ldots, a_{n-1}, a) = 0$ for all $a \in A_n$ and $\deg_{x_n} f < |A_n|$, the $n = 1$ case implies that $f(a_1, a_2, \ldots, a_{n-1}, x_n) = 0$ must be the zero polynomial. Hence $f_i(a_1, \ldots, a_{n-1}) = 0$ for

each $1 \leq i \leq n$ and each $(a_1, \ldots, a_{n-1}) \in \prod_{i=1}^{n-1} A_i$. Then, by the inductive hypothesis each f_i is the zero polynomial, so f is the zero polynomial. □

This lemma comprises the majority of the intellectual heavy lifting for our main theorem, and thus its proof will appear very simple in comparison to its powerful statement:

Theorem 2.2 (Generalized Combinatorial Nullstellensatz [7])**.** Let R be an integral domain, $n \geq 1$, and let $A_1, A_2, \ldots, A_n \subseteq R$ be finite and nonempty.
Let $f(\mathbf{x}) \in R[x_1, x_2, \ldots, x_n]$ be a polynomial and define $g_i(x_i) = \prod_{a \in A_i} (x_i - a)$ for $1 \leq i \leq n$. Then, $f(a_1, a_2, \ldots, a_n) = 0$ for all $\mathbf{a} \in \prod_{i=1}^{n} A_i$ if and only if there are polynomials $h_1(\mathbf{x}), h_2(\mathbf{x}), \ldots, h_n(\mathbf{x}) \in R[x_1, x_2, \ldots, x_n]$ such that

$$f(\mathbf{x}) = \sum_{i=1}^{n} g_i(x_i) h_i(\mathbf{x})$$

and

$$\deg(g_i h_i) \leq \deg(f) \text{ and } \deg_{x_j}(g_i h_i) \leq \deg_{x_j}(f_i)$$

for all $1 \leq i, j \leq n$.

Proof. First, assume there exist polynomials $h_1, \ldots, h_n \in R[x_1, \ldots, x_n]$ so that $f(\mathbf{x}) = \sum_{i=1}^{n} g_i(x_i) h_i(\mathbf{x})$ and the constraints on the degree of $g_i h_i$ hold. Then, it is clear $f(\mathbf{a}) = 0$ for each $\mathbf{a} \in \prod_{i=1}^{n} A_i$.

Conversely, suppose $f(a_1, \ldots, a_n) = 0$ for all $\mathbf{a} \in \prod_{i=1}^{n} A_i$. We wish to show that there are polynomials $h_1, \ldots, h_n$, such that $f(\mathbf{x}) = \sum_{i=1}^{n} g_i(x_i) h_i(\mathbf{x})$ together with the constraint on the degree of $g_i h_i$. For each $1 \leq j \leq n$, let $g_{ji} \in R$ so that:

$$g_j(x_j) = \prod_{a \in A_j} (x_j - a) = x_j^{|A_j|} - \sum_{i=0}^{|A_j|-1} g_{ji} x_j^i. \tag{2.1}$$

Hence, as $a_j \in A_j$ implies that $g_j(a_j) = 0$ we must have that $a_j^{|A_j|} = \sum_{i=0}^{|A_j|-1} g_{ij} a_j^i$. Now,

we define a new polynomial $\overline{f}$, such that $\overline{f}$ is the result of starting with the polynomial$f$ and applying a substitution of the form $x_j^{|A_j|} \mapsto \sum_{i=0}^{|A_j|-1} g_{ij} x_j^i$ for each $1 \leq j \leq n$euntil this is no longer possible (there are no powers of $x_j^{|A_j|}$ remaining). We see that $\deg_{x_i}\left(\overline{f}\right) < |A_i|$ for each i (as any monomial term of degree $|A_i|$ can be substituted for terms of lesser degree), and as $\overline{f}\left(\mathbf{a}\right) = f\left(\mathbf{a}\right) = 0$ for each $\mathbf{a} \in \prod_{i=1}^{n} A_i$ (this fact is trivial by the construction of f and $\overline{f}$), then by the preceding lemma we have that $\overline{f} = 0$. Next, consider the polynomial $f\left(\mathbf{x}\right) - \overline{f}\left(\mathbf{x}\right)$. Define $f_0 = f$ and f_i to be f after the i'th such substitution. Furthermore, let $N \in \mathbb{N}$ be such that $f_N = \overline{f}$. Then, the polynomial f_i is obtained by examining a term of f_{i-1} with a degree in x_j of at least $|A_j|$ and replacing an individual factor of $x_j^{|A_j|}$ by the sum as we defined earlier. For simplicity let us take the term $cx_1^{k_1}x_2^{k_2}\ldots x_n^{k_n} \cdot x_j^{|A_j|}$ (where $k_j \geq 0$ by our construction) and apply such a substitution. Then, we see that the difference

$$f_{i-1} - f_i = cx_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}\left(x_j^{|A_j|} - \sum_{i=0}^{|A_j|-1} g_{ji}x_j^i\right) = cx_1^{k_1}x_2^{k_2}\ldots x_n^{k_n} \cdot g_j\left(x_j\right)$$

by 2.1. Furthermore, as $f_N = \overline{f}$ we have that

$$f - \overline{f} = \left(f_0 - f_1\right) + \left(f_1 - f_2\right) + \ldots + \left(f_{N-1} - f_N\right).$$

Hence, $f = f - 0 = f - \overline{f} = \sum_{j=1}^{n} g_j\left(x_j\right) h_j$ where each $h_j \in R[x_1, x_2, \ldots, x_n]$ is simply the sum of all of these preceding terms $cx_1^{k_1}\ldots x_n^{k_n}$ as a result of these substitutions. Furthermore, we had by construction that $\deg g_j = |A_j| > \deg\left(\sum_{i=0}^{|A_j|-1} g_{ji}x_j^i\right)$, so we see that such a substitution will never increase the degree of our polynomial and hence $\deg f_i \leq \deg f$. Then, as $\deg g_j = |A_j|$, we see that

$$\deg\left(cx_1^{k_1}\ldots x_n^{k_n}g_j(x_j)\right) \leq \deg f_{i-1} \leq \deg f.$$

As each h_j is simply the sum of such terms, $cx_1^{k_1} \dots x_n^{k_n}$, we may substitute its degree to yield $\deg(g_j h_j) \leq \deg f$.

Lastly, we show this holds for projected degree as well. Note that as we are replacing a term g_j with $\deg_{x_k}(g_j) = 0$, and as each h_j with $\sum_{i=0}^{|A_j|-1} g_{ji} x_j^i$ also has projected degree 0, the overall degree in x_k will not increase after i substitutions. Hence for $k \neq j$, $\deg_{x_k}\left(cx_1^{k_1} \dots x_n^{k_n} g_j(x_j)\right) \leq \deg_{x_k}(f_{i-1}) \leq \deg_{x_k}(f)$. Moreover, if $k = j$, the same argument shows the projected degrees decrease. These facts yield $\deg_{x_k}\left(cx_1^{k_1} \dots x_n^{k_n} g_j\right) \leq \deg_{x_k}(f)$. And, as each h_j is simply the sum of these remaining terms, we see $\deg_{x_k}(h_j) + \deg_{x_k}(g_j) \leq \deg_{x_k}(f)$ for each $1 \leq j, k \leq n$. □

This theorem is perhaps too general and too powerful for use in proving our simpler results. As a corollary, many authors include a weaker second statement of the theorem, where the splitting of a polynomial is replaced by a constraint on the cardinality of the set on which $f(\mathbf{x}) = 0$.

Theorem 2.3 (Combinatorial Nullstellensatz [7])**.** Let R be an integral domain, $n \geq 1$, and $A_1, A_2, \dots, A_n \subseteq R$ be finite and nonempty, with $f(\mathbf{x}) \in R[x_1, x_2, \dots, x_n]$ being a polynomial. Suppose

$$[x_1^{d_1} x_2^{d_2} \dots x_n^{d_n}] f(\mathbf{x}) \neq 0$$

and that $\deg f = \sum_{i=1}^n d_i$ with $0 \leq d_i \leq |A_i| - 1$. Then, there exists an element $\mathbf{a} \in \prod_{i=1}^n A_i$ such that $f(\mathbf{a}) \neq 0$. That is, given a nontrivial "maximal degree" monomial of f such that the degree of this monomial in each variable, x_i, is strictly less than the size of the corresponding set A_i, f cannot be zero on the whole of the product of the A_i.

This is in essence a generalization of the Fundamental theorem of Algebra and it is precisely this simple statement about the number of zeroes of a particular polynomial

which provides our combinatorial power. The proof follows rather directly from the generalized version as follows:

Proof. Let $g_i = \prod_{a \in A_i} (x_i - a)$ for $1 \leq i \leq n$ and suppose indirectly that $f(\mathbf{a}) = 0$ for all $\mathbf{a} \in \prod_{i=1}^{n} A_i$ with $\deg(f) = \sum_{i=1}^{n} d_i$ and $\left[x_1^{d_1} \dots x_n^{d_n}\right] f(\mathbf{x}) \neq 0$. Now, $x_1^{d_1} \dots x_n^{d_n}$ is a maximal degree monomial. Then, theorem 2.1 yields polynomials, which we will denote as $h_1, h_2, \dots, h_n \in R[x_1, x_2, \dots, x_n]$ such that $f(\mathbf{x}) = \sum_{i=1}^{n} g_i(x_i) h_i(\mathbf{x})$ and $\deg(g_i h_i) \leq \deg(f)$ for each $1 \leq i \leq n$. Now let us examine the nature of $[x_1^{d_1} \dots x_n^{d_n}] f(\mathbf{x})$. As this is a maximal degree monomial of f, then only maximal degree monomials of $h_i(\mathbf{x}) g_i(x_i)$ can contribute to its coefficient in f as $\deg(h_i g_i) \leq \deg f$. Since $\deg(g) = |A_i| > d_i$, we find $\deg_{x_i}(h_i g_i) \geq |A_i| > d_i$. So, all maximal degree monomials, M, of f must have $\deg_{x_j}(M) \geq |A_i|$ for some $1 \leq j \leq n$. So, $x_1^{d_1} \dots x_n^{d_n}$ cannot be a maximal degree monomial since $d_i < |A_i|$ for all $1 \leq i \leq n$, a contradiction. Thus, we must have some $\mathbf{a} \in \prod_{i=1}^{n} A_i$ so that $f(\mathbf{a}) \neq 0$. □

Our last version of the Combinatorial Nullstellensatz will examine what happens when f vanishes over not all, but most (in a certain set-theoretic perspective) of the members of the product. This is known as the Punctured Combinatorial Nullstellensatz and it builds on the original generalized version. The proof will involve division of polynomials of many variables, so let us first examine the nature of such an operation.

Ball and Serra's Punctured Nullstellensatz

Sometimes we will not have polynomials which are zero over the whole of a set, but just on part. These conditions yield the Punctured Nullstellensatz. But, before we may state the theorem itself, we must state a result about the well-behavedness of multivariate polynomial division.

Lemma 2.2 (Multivariate Polynomial Division [7])**.** Let R be an integral domain and let $g_1(x_1), \ldots, g_k(x_k) \in R[x_1, x_2, \ldots, x_n]$ be polynomials of one variable with leading coefficient 1 for $1 \leq k \leq n$. Then,

1. If $f \in \sum_{i=1}^{k} R[x_1, \ldots, x_n] \cdot g_i(x_i)$ is a nonzero polynomial in the ideal generated by $g_1(x_1), \ldots, g_k(x_k)$ over $R[x_1, \ldots, x_n]$, then $\deg_{x_i}(f) \geq \deg(g_i)$ for some $1 \leq i \leq k$.

2. For a polynomial $f \in R[x_1, \ldots, x_n]$ there are $w(\mathbf{x}), h_1(\mathbf{x}), \ldots, h_k(\mathbf{x}) \in R[x_1, \ldots, x_n]$ such that

$$f(\mathbf{x}) = \sum_{i=1}^{k} h_i(\mathbf{x}) g_i(x_i) + w(\mathbf{x}).$$

with $\deg_{x_j}(w) < \deg(g_j)$, $\deg_{x_j}(g_i h_i) \leq \deg_{x_j}(f)$, $\deg(g_i h_i) \leq \deg(f)$, $\deg_{x_j}(w) \leq \deg_{x_j}(f)$, and $\deg(w) \leq \deg(f)$ for all $1 \leq i \leq k$, $1 \leq j \leq n$.

Furthermore, the polynomial $w(\mathbf{x})$ is unique. We call the polynomial $w(\mathbf{x})$ the **minimal coset representative**. .

Proof. First, we show the existence of the polynomials h_i and w given in (2). As we did before, we let $g_{ji} \in R$ so that $g_j(x_j) = x_j^{\deg(g_j)} - \sum_{i=0}^{\deg(g_j)-1} g_{ji} x_j^i$ for each $j \in [1, k]$.

First, consider g_1. It is clear by normal univariate polynomial division that we can write $f(\mathbf{x}) = A_1(\mathbf{x}) x_1^{\deg(g_1)} + B_1(\mathbf{x})$ where $\deg_{x_1}(B_1) < \deg(g_1)$,
$\deg(A_1 g_1) = \deg\left(A_1 x_1^{\deg(g_1)}\right) \leq \deg(f)$, $\deg(B_1) \leq \deg(f)$,

$\deg_{x_i}\left(A_1 x_1^{\deg(g_1)}\right) \leq \deg_{x_i}(f)\deg_{x_i}(B_1) \leq \deg_{x_i}(f)$ for all $1 \leq i \leq n$. Then, substituting $g_1(x_1) + \sum_{i=0}^{\deg(g_1)-1} g_{1i}x_1^i$ in place of $x_1^{\deg(g_1)}$, we obtain

$$f(\mathbf{x}) = A_1(\mathbf{x})\, g_1(x_1) + \big(A_1(\mathbf{x}) \sum_{i=0}^{\deg(g_1)-1} g_{1i}x^i + B_1(\mathbf{x})\big).$$

Denote the second term to be $f_1(\mathbf{x})$, so $f(\mathbf{x}) = A_1(\mathbf{x})\, g_1(x_1) + f_1(\mathbf{x})$ and note that the previous constraints on degree imply $\deg_{x_i}(f_1) \leq \deg_{x_i}(f)$ for all $1 \leq i \leq n$ and $\deg(f_1) \leq \deg(f)$. We repeat this process inductively, assuming we have already constructed $f_j(\mathbf{x})$, $1 \leq j < k$, so that $f = \sum_{i=1}^{j} A_i(\mathbf{x})\, g_i(x_i) + f_j(\mathbf{x})$ we find $A_{j+1}, B_{j+1} \in R[x_1, \ldots, x_n]$ so that
$f(\mathbf{x}) = \sum_{i=1}^{j+1} A(\mathbf{x})\, g_i(x_i) + \left(A_{j+1}(\mathbf{x}) \sum_{i=0}^{\deg(g_{j+1})-1} g_{(j+1)i}x_{j+1}^i + B_{j+1}(\mathbf{x})\right)$ with $\deg_{x_{j+1}}(B_{j+1}) < \deg(g_{j+1})$, $\deg(A_{j+1}g_{j+1}) \leq \deg(f_j)$, $\deg(B) \leq \deg(f_j)$, $\deg_{x_i}\left(Ax_{j+1}^{\deg(g_{j+1})}\right) \leq \deg_{x_i}(f_j)$, and $\deg_{x_i}(B) \leq \deg_{x_i}(f_{j+1})$ for all $1 \leq i \leq n$. Then, we denote $f_{j+1} = A_{j+1}(\mathbf{x}) \sum_{i=0}^{\deg(g_{j+1})-1} g_{(j+1)i}x_{j+1}^i + B_{j+1}(\mathbf{x})$. Hence, $f = \sum_{i=1}^{j+1} A_i(\mathbf{x})\, g_i(x_i) + f_{j+1}(\mathbf{x})$.

Repeating until the case $j = k$ yields $f(\mathbf{x}) = \sum_{i=1}^{k} A_i(\mathbf{x})\, g_i(x_i) + f_k(\mathbf{x})$. Labeling $A_i = h_i$ and $f_k = w$, we obtain the desired result of (2) with all of the desired constraints on degree holding true since they held true at each step of the construction.

Next, we show (1) implies $f_n(\mathbf{x}) = w(\mathbf{x})$ is unique. Suppose $w(\mathbf{x})$ is not unique, that is,

$$f(\mathbf{x}) = \sum_{i=1}^{k} h_i(\mathbf{x})\, g_i(x_i) + w(\mathbf{x}) = \sum_{i=1}^{k} \overline{h}_i(\mathbf{x})\, g_i(x_i) + v(\mathbf{x})$$

for polynomials $h_1, \ldots, h_k, \overline{h}_1, \ldots, \overline{h}_k, w, v \in R[x_1, \ldots, x_n]$ with $w(\mathbf{x}) \neq v(\mathbf{x})$ and the degree requirements of (2) satisfied. Denote $\overline{f} = f + (g_1(x_1), \ldots, g_k(x_k))$, where $(g_1(x_1) \ldots g_k(x_k))$ is the ideal generated by the g_i's. Then, $w, v \in \overline{f}$, that is w and v are coset representatives of $\overline{f}$. Since $w \neq v$, and ideals form an abelian group under addition, we have $w - v \in (g_1(x_1), \ldots, g_k(x_k)) = \sum_{i=1}^{k} R[x_1, \ldots, x_n]\, g_i(x_i)$ a nonzero polynomial. Then, (1) implies $\deg_{x_i}(w - v) \geq \deg(g_i)$ for some $1 \leq i \leq k$, but since

$\deg_{x_i}(w-v) \leq \max\{\deg_{x_i}(w), \deg_{x_i}(v)\} < \deg_{x_i}(g_i)$ by the first degree constraint of (2), we have a contradiction. Thus, (1) and (2) imply the polynomial w is unique.

Finally, we show that (1) is indeed true. If $k = 1$ then the claim is obvious since $f \neq 0$, and $f = h_1(\mathbf{x}) g_1(x_1)$ for some $h_1 \in R[x_1, \ldots, x_n]$ nonzero. So, we proceed by induction. Assuming the claim is already shown for $k-1$ polynomials g_i, we prove the claim for k polynomials g_i.

Let $f(\mathbf{x}) = \sum_{i=1}^{k} v_i(\mathbf{x}) g_i(x_i)$, with $v_i(\mathbf{x}) \in R[x_1, \ldots, x_n]$. We can assume that $v_j(\mathbf{x}) \notin (g_1(x_1), \ldots, g_{j-1}(x_{j-1}))$, for any $1 \leq j \leq k$. Otherwise, if $v_j g_j = \sum_{i=1}^{j-1} u_i g_i(x_i)$ for some polynomials $u_i \in R[x_1, \ldots, x_n]$ we can replace v_i with $v_i + u_i$ for each $1 \leq i \leq k$. We can then apply the inductive hypothesis to see the claim is true.

So, assuming all $v_j \neq 0$ and each v_j is not contained in the ideal $(g_1(x_1), \ldots, g_{j-1}(x_{j-1}))$, we find $v_k \not\equiv 0 \mod (g_1(x_1), \ldots, g_{k-1}(x_{k-1}))$. Moreover, letting $\overline{h} \in h + (g_1(x_1), \ldots, g_{k-1}(x_{k-1}))$denote the minimal coset representative for any polynomials $h \in R[x_1, \ldots, x_n]$, we find $\overline{v_i g_i} = 0$ for all $1 \leq i \leq k-1$, so

$$\overline{f} = \overline{v_k(\mathbf{x}) + g_k(x_k)}.$$

Next, note that $\deg_{x_k}\left(\overline{f}\right) \leq \deg_{x_k}(f)$, by applying the definition of $\overline{f}$. If we assume indirectly that $\deg_{x_k}(f) < \deg_{x_k}(g_k(x_k))$, we attain the inequality,

$$\deg_{x_k}\left(\overline{v_k(\mathbf{x}) g_k(x_k)}\right) = \deg_{x_k}\left(\overline{f}\right) \leq \deg_{x_k}(f) < \deg_{x_k}(g_k). \tag{2.2}$$

But, since g_j is a polynomial in only the variable x_j for each $1 \leq j \leq k$, it follows that $\overline{v_k(\mathbf{x}) g_k(x_k)} = \overline{v_k(\mathbf{x})} \cdot \overline{g_k(x_k)}$ since v_k is not in the ideal $(g_1(x_1), \ldots, g_{k-1}(x_{k-1}))$ as we noted earlier. Finally, we note $\overline{g_k(x_k)} = g_k(x_k)$ so, since we assumed earlier $v_k \neq 0$, we have $\deg_{x_k}\left(\overline{v_k(\mathbf{x})} g_k(x_k)\right) \geq \deg_{x_k}(g_k(x_k))$ by the increasing nature of polynomial

degree under nonzero multiplication. This is a contradiction with (2.2), so (1) holds. Thus, uniqueness of w holds and we see the lemma is thus proven. $\square$

Theorem 2.4 (Punctured Combinatorial Nullstellensatz [7])**.** Let R be an integral domain and let $A_1, A_2, \ldots, A_n \subset R$ be finite and nonempty. Furthermore, for each $1 \leq i \leq n$, let $B_i \subseteq A_i$ be nonempty.

Let $f(\mathbf{x}) \in R[x_1, x_2, \ldots, x_n]$ be a polynomial and set $g_i(x_i) = \prod_{a \in A_i}(x_i - a)$ and $l_i(x_i) = \prod_{b \in B_i}(x_i - b)$. If

$$f(\mathbf{a}) = 0 \text{ for all } \mathbf{a} \in \left(\prod_{i=1}^{n} A_i\right) \setminus \left(\prod_{i=1}^{n} B_i\right) \tag{2.3}$$

but there exists a $\mathbf{b} \in \prod_{i=1}^{n} B_i$ such that $f(\mathbf{b}) \neq 0$, then there are polynomial $h_i \in R[x_1, x_2, \ldots, x_n]$ with $1 \leq i \leq n$ such that

$$f(\mathbf{x}) = \sum_{i=1}^{n} g_i(x_i) h_i(\mathbf{x}) + w(\mathbf{x}) \text{ with } w(\mathbf{x}) = u(\mathbf{x}) \prod_{i=1}^{n} \frac{g_i(x_i)}{l_i(x_i)}. \tag{2.4}$$

with the following conditions holding:

$\deg(w) \leq \deg(f), \deg_{x_j}(w) \leq \deg_{x_j}(f)$ for all $1 \leq j \leq n$, $\deg_{x_i}(w) < |A_i|$, $\deg(g_i h_i) \leq \deg(f)$ for $1 \leq i \leq n$ and $\deg_{x_j}(g_i h_i) \leq \deg_{x_j}(f)$ for $1 \leq i, j \leq n$. Consequently $\sum_{i=1}^{n}(|A_i| - |B_i|) \leq \deg(w) \leq \deg(f)$.

Proof. Lemma 2.2 guarantees there to be polynomials

$$w(\mathbf{x}), h_1(\mathbf{x}), \ldots, h_n(\mathbf{x}) \in R[x_1, x_2, \ldots, x_n]$$

of the desired form and for which the proper conditions hold (the degree restrictions from implication (2) of the lemma). Our first task, then, is to ensure that the form of $w(\mathbf{x})$ is that of (2.4). First, let $1 \leq i \leq n$ and without loss of generality select $i = 1$. We consider $w(\mathbf{x}) l_1(x_1)$. Then as $f(\mathbf{a}) = \sum_{i=1}^{n} g_i(a_i) h_i(\mathbf{a}) = 0$ for all

$\mathbf{a} = (a_1, \ldots, a_n) \in \prod_{i=1}^{n} A_i \setminus \prod_{i=1}^{n} B_i$, we see $w(\mathbf{a}) = 0$ for all the same $\mathbf{a}$'s. Since $l_1(a_1) = 0$ for all $a_1 \in B_1$, we then have $w(\mathbf{a}) l_1(a_1) = 0$ for all $\mathbf{a} \in \prod_{i=1}^{n} A_i$. Applying Theorem 2.2 yields polynomials $v_1, \ldots, v_n \in R[x_1, \ldots, x_n]$ such that

$$w(\mathbf{x}) l_1(x_1) = \sum_{i=1}^{n} g_i(x_i) v_i(\mathbf{x}). \tag{2.5}$$

Now, letting $(v_1(x_1), \ldots, v_k(x_k))$ denote the ideal generated by the v_i's, $1 \leq i \leq k$, we see, by the same construction as in the previous lemma, we can assume without loss of generality that each $v_i(\mathbf{x}) \notin (v_1(\mathbf{x}), \ldots, v_{i-1}(\mathbf{x}))$ for all $1 \leq i \leq n$ where $v_i \neq 0$. Next, since $\deg_{x_n}(w) < \deg(g_n) = |A_n|$ by lemma 2.2 we have $\deg(w(\mathbf{x}) l_1(x_1)) < |A_n|$ for all $n > 1$.

Now, once again we let $\overline{h} \in h + (g_1(x_1), \ldots, g_{n-1}(x_{n-1}))$ be the minimal coset representative for a polynomial $h \in R[x_1, \ldots, x_n]$. Then, applying the same arguments as in lemma 2.2, we find $\overline{w(\mathbf{x}) l_1(x_1)} = \overline{g_n(x_n) v_n(\mathbf{x})}$. Hence, since $\overline{w(\mathbf{x}) l_1(x_1)}$ is the minimal coset representative, we have $\deg_{x_n}\left(\overline{w(\mathbf{x}) l_1(x_1)}\right) \leq \deg_{x_n}(w(\mathbf{x}) l_1(x_1))$. So, for all $n \geq 2$

$$\deg_{x_n}\left(\overline{v_n(\mathbf{x}) g_n(x_n)}\right) = \deg_{x_n}\left(\overline{w(\mathbf{x}) l_1(x_1)}\right) \leq \deg_{x_n}(w(\mathbf{x}) l_1(x_1)) < |A_n| = \deg_{x_n}(g_n). \tag{2.6}$$

Moreover, since $g_n(x_n) = \overline{g_n(x_n)}$, we find $\overline{v_n(\mathbf{x}) g_n(x_n)} = \overline{v_n(\mathbf{x})} g_n(x_n)$, so if $\overline{v_n(\mathbf{x})} \neq 0$ then $\deg_{x_n}\left(\overline{v_n(\mathbf{x}) g_n(x_n)}\right) \geq \deg_{x_n}(g_n(x_n))$, a contradiction with (2.6). Thus, $\overline{v_n(\mathbf{x})} = 0$ and, since $\overline{v_n(\mathbf{x})} \notin (v_1(x_1), \ldots, v_{n-1}(x_{n-1}))$ we must have $v_n(\mathbf{x}) = 0$. So, $w(\mathbf{x}) l_1(x_1) = \sum_{i=1}^{n-1} g_i(x_i) v_i(\mathbf{x})$. Then, the same argument will hold for all $j > 1$, so we may repeat it until $j = 2$ to see $v_i(\mathbf{x}) = 0$, $2 \leq i \leq n$. Hence, $w(\mathbf{x}) l_1(x_1) = g_1(x_1) v_1(\mathbf{x})$, so $g_1(x_1) \mid w(\mathbf{x}) l_1(x_1)$. And, since $B_1 \subseteq A_1$, we know $l_1(x_1) \mid g_1(x_1)$, so $\frac{g_1(x_1)}{l_1(x_1)} \mid w(\mathbf{x})$.

Since we chose $i = 1$ arbitrarily, we have $l_i(x_i) \mid g_i(x_i)$ for all $1 \leq i \leq n$ and $\frac{g_i(x_i)}{l_i(x_i)} \mid w(\mathbf{x})$. Next, let F be the quotient field of R, so theorem 1.3 implies $F[x_1, \ldots, x_n]$

is a unique factorization domain. Since each $\frac{g_i(x_i)}{l_i(x_i)}$ is in a separate variable we see they can have no overlap in terms. Hence $\prod_{i=1}^{n} \frac{g_i(x_i)}{l_i(x_i)} \mid w(\mathbf{x})$ over $F[x_1, \ldots, x_n]$. That is, there is a $u(\mathbf{x}) \in F[x_1, \ldots, x_n]$ so that

$$w(\mathbf{x}) = u(\mathbf{x}) \prod_{i=1}^{n} \frac{g_i(x_i)}{l_i(x_i)}. \tag{2.7}$$

Since each $\frac{g_i(x_i)}{l_i(x_i)}$ is monic and univariate, and $w(\mathbf{x}), g_i(x_i), l_i(x_i) \in R[x_1, \ldots, x_n]$, then Theorem 1.4 implies $u(\mathbf{x}) \in R[x_1, \ldots, x_n]$. This shows that w is indeed of the form desired in (2.4), so all that remains to be shown is $\sum_{i=1}^{n} (|A_i| - |B_i|) \leq \deg(w)$.

If $w = 0$ then (2.4) implies $f(\mathbf{a}) = 0$ for all $\mathbf{a} \in \prod_{i=1}^{n} A_i$ since this is the property of the g_i's. This is a contradiction as there was atleast one $\mathbf{b} \in \prod_{i=1}^{n} B_i$ so that $f(\mathbf{b}) \neq 0$. So, we can assume $w \neq 0$, and since each $g_i \neq 0$, $1 \leq i \leq n$, we have $u \neq 0$. So,

$$\deg(w(\mathbf{x})) = \deg(u(\mathbf{x})) + \deg\left(\prod_{i=1}^{n} \frac{g_i(x_i)}{l_i(x_i)}\right) \geq \deg\left(\prod_{i=1}^{n} \frac{g_i(x_i)}{l_i(x_i)}\right) = \sum_{i=1}^{n} (|A_i| - |B_i|).$$

This inequality follows from the definitions of g_i and l_i, namely the fact that $\frac{g_i(x_i)}{l_i(x_i)} = \prod_{a \in A_i \setminus B_i} (x_i - a)$ and this completes the proof. □

With all three Nullstellensatz now stated and proven, we will move on to an examination of several smaller combinatorial proofs and a larger proof, the q-dyson conjecture, which rely on these results.

Chapter 3

Simple Combinatorial Proofs

Sumsets

Now, with our the Nullstellensatz stated and proven, let us examine a few simple results concerning sumsets. First though, we must define what a sumset is.

Definition 3.1 (Sumsets)**.** Let $A, B \subseteq G$ be subsets of an abelian group G.

- We construct a new set $A + B$, called the **sumset** of A and B, by $A + B = \{a + b : a \in A, b \in B\}$
- We construct another new set $A \oplus B$, called the **restricted sumset** of A and B, by $A \oplus B = \{a + b : a \in A, b \in B, a \neq b\}$
- For a polynomial $h \in C_p[x_1, x_2]$ we construct a third new set $A \,{}_h\!\oplus B$, called the **h-restricted sumset** of A and B, by

$$A \,{}_h\!\oplus B = \{a + b : a \in A, b \in B, h(a, b) \neq 0\}$$

- Let $A_1, \ldots, A_n \subseteq G$ be subsets, and $h \in C_p[x_1, \ldots, x_n]$ a polynomial. We construct the h-restricted sumset in the same way and denote it

$$\,{}_h\!\bigoplus_{i=1}^{n} A_i = \{\sum_{i=1}^{n} a_i : a_i \in A_i, 1 \leq i \leq n, h(a_1, \ldots, a_n) \neq 0\}.$$

It is worth noting that this notation overlaps heavily with that of the direct sum. For this reason all uses of $\oplus$ in this chapter will refer exclusively to the sumset, and all uses outside of this chapter (namely in chapter 6) will refer to the direct sum.

Our first Theorem, the Cauchy-Davenport Theorem, has been known for quite some time as the name would suggest. This proof invoking the combinatorial

nullstellensatz, however, is relatively new, first appearing in Alon's original paper on the subject.

Theorem 3.1 (Cauchy-Davenport Theorem [1])**.** Given a prime p and nonempty $A, B \subseteq C_p$, then $|A+B| \geq \min\{p, |A|+|B|-1\}$.

Proof. Suppose $|A|+|B| > p$. Then, for any element $x \in C_p$, $(A) \cap (x-B) \neq \varnothing$. Hence, $A+B = C_p$ (since, if $a = x-b$ for $a \in A$ and $b \in B$, we have $x = a+b$, so $x \in A+B$).. Thus, let us assume $|A|+|B| \leq p$ and suppose indirectly that $|A+B| \leq |A|+|B|-2$. Let $C \subseteq C_p$ so that $A+B \subseteq C$ with $|C| = |A|+|B|-2$. Next, define $f(x,y) = \prod_{c \in C}(x+y-c)$ and note that we must have $f(a,b) = 0$ for all $(a,b) \in A \times B$ as $A+B \subseteq C$. Now, note that $\deg(f) = |C| = |A|+|B|-2$, and hence $[x^{|A|-1}y^{|B|-1}]f(x,y) = \binom{|A|+|B|-2}{|A|-1} \neq 0$ as $|A|+|B|-2 < p$. Hence, by theorem 2.3, we must have a pair $(a,b) \in A \times B$ such that $f(a,b) \neq 0$, a contradiction. So, we see the theorem is true. □

The next result naturally generalizes the Cauchy-Davenport theorem to h-restricted sumsets.

Proposition 3.1 ([1])**.** Let p be a prime, let $h(x_1..,x_k) \in C_p[x_1,\ldots,x_k]$ be a polynomial, and let $A_1,\ldots,A_k \subseteq C_p$ be nonempty. Define $m = \sum_{i=1}^{k}|A_i| - \deg(h) - k$. If $[x_1^{|A_1|-1}\ldots x_k^{|A_k|-1}]((\sum_{i=1}^{k}x_i)^m \cdot h(\mathbf{x})) \neq 0$, then

$$\left|{}_h\bigoplus_{i=1}^{k}A_i\right| \geq m+1.$$

Consequently, $m < p$.

Proof. Let $A_0,\ldots,A_k \subseteq C_p$ and $h(x_0,\ldots,x_k) \in C_p[x_0,\ldots,x_k]$. We will prove the claim for $k+1$ sets, thus proving it for k sets since k is arbitrary. Suppose indirectly that the inequality does not hold. Then choose elements $e_1,\ldots,e_m$, which are not necessarily

distinct, so that ${}_h\bigoplus_{i=0}^{k} A_i \subseteq \{e_1, \ldots, e_m\}$. Let $c_i = |A_i| - 1$ for each $0 \leq i \leq k$ and let $Q(\mathbf{x}) = h(\mathbf{x}) \prod_{j=1}^{m} \left(\sum_{i=0}^{k} x_i - e_j \right)$. By our construction we must have that $Q(\mathbf{x}) = 0$ for all $\mathbf{x} \in \prod_{i=0}^{k} A_i$ as either $h(\mathbf{x}) = 0$ or $\sum_{i=0}^{k} x_i \in {}_h\bigoplus_{i=0}^{k} A_i \subseteq \{e_1, \ldots, e_m\}$. Furthermore $\deg(Q) = m + \deg(h) = \sum_{i=0}^{k} c_i$ by construction. Next, we see $[x_0^{c_0} \ldots c_k^{c_k}]Q \neq 0$ holds by hypothesis.

Therefore, applying theorem 2.3 yields an $\mathbf{a} \in A$ such at $Q(\mathbf{a}) \neq 0$, a contradiction. So, $p \geq \left| {}_h\bigoplus_{i=0}^{k} A_i \right| \geq m + 1$. Thus, we have $m < p$. □

With this result on h-restricted sumsets proven, we now prove superior bounds on the standard restricted sumsets. Note that the standard restricted sumset is equivalent to an h-restricted sumset with the polynomial $h(x) = \prod_{1 \leq i,j \leq n : i \neq j} (a_i - a_j)$.

Theorem 3.2 (Restricted Sumset Theorem[1])**.** Let p be prime and let $A_1, \ldots, A_k \subseteq C_p$ be nonempty with $|A_i| \neq |A_j|$ for any $i \neq j$. If $\sum_{i=1}^{k} |A_i| \leq p + \binom{k+2}{2} - 1$, then

$$\left| \bigoplus_{i=1}^{k} A_i \right| \geq \sum_{i=1}^{k} |A_i| - \binom{k+2}{2} + 1.$$

In order to prove this theorem, let us first state and prove two lemmas concerning the coefficient of a particular polynomial.

Lemma 3.1 (Vandermonde determinant)**.** [10] Let F be a field, and A be the $k \times k$ matrix over $F[x_1, \ldots, x_k]$ with

$$A = \begin{bmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{k-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_k & x_k^2 & \ldots & x_k^{k-1} \end{bmatrix}.$$

Then, $\det(A) = \prod_{k \geq i > j \geq 1} (x_i - x_j) = \sum_{\sigma \in S_k} (-1)^{\operatorname{sgn}(\sigma)} \prod_{i=1}^{k} x_i^{\sigma(i)}$, where S_k is the permutation group on k elements. This polynomial is called the Vandermonde determinant.

Proof. First, note that $\det(A) \in F[x_1, \ldots, x_k]$. Next, recall that one summand of the determinant will be produce of the diagonal of A, which is a polynomial of degree $\sum_{i=0}^{k-1} i = \frac{k(k-1)}{2}$, and since each x_i^j is unique as a polynomial, we see there is no chance this summand will cancel with any other. Moreover, all other summands of $\det(A)$ will also consist of the product of one element from each column. Thus, it is clear $\deg(\det(A)) = \frac{k(k-1)}{2}$. Next, if $x_i = x_j$ for some $i \neq j$ we would have the rows of A not being linearly independent as there would be duplicates, hence $\det(A) = 0$ in this case. So, we must have $(x_i - x_j) \mid \det(A)$. Since $F[x_1, \ldots, x_k]$ is a unique factorization domain by theorem 1.3 and the factors $(x_j - x_i)$ will have no overlap, we see $\prod_{1 \leq i < j \leq k} (x_j - x_i) \mid \det(A)$. So, $\det(A) = F \prod_{1 \leq i < j \leq n} (x_j - x_i)$ for some $F \in F[x_1, \ldots, x_k]$. Since $\deg\left(\prod_{1 \leq i < j \leq k} (x_j - x_i)\right) = \frac{k(k-1)}{2}$, we see $\deg(F) = 0$ and as we noted earlier, each product over the diagonals will be distinct with each other and with coefficient equal to 1, so all terms in $\det(A)$ will have coefficient 1. Since all terms in $\prod_{1 \leq i < j \leq n} (x_j - x_i)$ also have coefficient 1, we see $F = 1$, so the first equality is shown. From here it is routinely checked that the second equality follows. $\square$

Lemma 3.2. [3] Let $c_1, \ldots, c_k \in \mathbb{Z}$ be nonnegative and define $m = \sum_{1=0}^{k} c_i - \binom{k}{2}$ (it is trivial that m is nonnegative). Then,

$$C = [x_1^{c_1} \ldots x_k^{c_k}] \left(\left(\sum_{i=1}^{k} x_i \right)^m \prod_{k \geq i > j \geq 1} (x_i - x_j) \right) = \frac{m!}{c_1! c_1! \ldots c_k!} \prod_{k \geq i > j \geq 1} (c_i - c_j).$$

Proof. Once again, we prove the case for $k+1$ nonnegative integers, implying the case for k. Let $c_0, \ldots, c_k \in \mathbb{Z}$ and $m = \sum_{i=0}^{k} c_i - \binom{k+1}{2}$. Then, $\prod_{1 \leq j < i \leq k} (x_i - x_j)$ is the Vandermonde determinant, which lemma 3.1 prove is equal to $\sum_{\sigma \in S_{k+1}} (-1)^{\mathrm{sgn}(\sigma)} \prod_{i=0}^{k} x_i^{\sigma(i)}$.

It follows that the coefficient $C = \sum_{\sigma \in S_{k+1}} (-1)^{\mathrm{sgn}(\sigma)} \frac{m!}{(c_0 - \sigma(0))! \ldots (c_k - \sigma(k))!}$. Now, for $r \geq 1$ denote $\varphi_r(s) = s(s-1)\ldots(s-(r-1))$ and $\varphi_0(s) = 1$. Next, note that $\prod_{k \geq i > j \geq 0} (c_i - c_j)$ is precisely the vandermonde determinant on the c_i rather than the x_i. Finally, let $A = \left((c_i)_j \right)$ be the $k \times k$ matrix with $(c_i)_j$ in the i, j'th position for $0 \leq i, j \leq k$. Sufficient subtraction of linear combinations from the vandermonde matrix on the c_i yields A, so their determinants are equal. Hence, it follows that

$$\begin{aligned}
\frac{m!}{c_0! \ldots c_k!} \prod_{k \geq i > j \geq 0} (c_i - c_j) &= \frac{m!}{c_0! \ldots c_k!} \det(A) \\
&= \frac{m!}{c_0! \ldots c_k!} \sum_{\sigma \in S_{k+1}} (-1)^{\mathrm{sgn}(\sigma)} (c_0)_{\sigma(0)} \ldots (c_k)_{\sigma(k)} \\
&= \sum_{\sigma \in S_{k+1}} (-1)^{\mathrm{sgn}(\sigma)} \frac{m!}{(c_0 - \sigma(0))! \ldots (c_k - \sigma(k))!} \\
&= C.
\end{aligned}$$

□

With this out of the way, we now prove theorem 3.2:

Proof of Theorem 3.2. For this proof we will take the aforementioned

$$h(\mathbf{x}) = \prod_{0 \le i < j \le k} (x_i - x_j).$$

Now, let us define $c_i = |A_i| - 1$ and $m = \sum_{i=0}^{k} c_i - \binom{k+1}{2}$. Rearranging the assumptions of this theorem yields $\sum_{i=0}^{k} |A_i| - \binom{k+2}{2} + 1 \le p$ and, applying the trivial combinatorial identity $\binom{k+2}{2} = \binom{k+1}{2} + (k+1)$ yields

$\sum_{i=0}^{k} c_i - \binom{k+1}{2} + 1 = m + 1 \le p$ (hence $m < p$). Then

$$[x_0^{c_0} \dots x_k^{c_k}] \left(\left(\sum_{i=0}^{k} x_i \right) h \right) = \frac{m!}{c_0! \dots c_k!} \prod_{0 \le i < j \le k} (c_i - c_j).$$

We know this product to be nonzero modulo p as $c_i \neq c_j$ for $i \neq j$ by construction and $m < p$. Finally, as the coefficient is nonzero and as $\deg(h) = \binom{k+2}{2}$ (as there are $k+2$ possible x_i's and each term of the product will contain two distinct x_i's so there are $\binom{k+2}{2}$ terms each of degree 1), we have $m = \sum_{i=0}^{k} c_i - \deg(h)$. Hence, applying theorem 3.1 yields $\left| \oplus_h \sum_{i=0}^{k} A_i \right| \ge m + 1 = \sum_{i=0}^{k} |A_i| - \binom{k+2}{2} + 1$. □

A special case of theorem 3.2, when it is taken over only 2 sets, yields an even tighter bound. This result was originally conjectured by Erdős and Heilbronn and is named as such. First, though, we must prove another lemma

Lemma 3.3 ([7])**.** Let F be a field, $n \ge 1$, and $A_1, \dots, A_n \subseteq F$ be finite nonempty subsets. Let $f(\mathbf{x}) \in F[x_1, \dots, x_n]$ be a polynomial such that $\deg(f) \le \sum_{i=1}^{n} |A_i| - n$ and

$$\left[x_1^{|A_1|-1} \dots x_n^{|A_n|-1} \right] \left(f(\mathbf{x}) \left(\sum_{i=1}^{n} x_i \right)^{\sum_{i=1}^{n} |A_i| - n - \deg(f)} \right) \neq 0. \tag{3.1}$$

Then,

$$\left| {}_f\bigoplus_{i=1}^{n} A_i \right| \ge \sum_{i=1}^{n} |A_i| - n - \deg(f) + 1.$$

Proof. First of all, we can assume without loss of generality that $|F| = \infty$, else we can just replace F with an infinite field extension. Denote ${}_f\bigoplus_{i=1}^n A_i = B'$. Then, suppose indirectly that $B \leq \sum_{i=1}^n |A_i| - n - \deg(f)$ (in contradiction to the lemma). Since F is infinite, we can always append new elements to B' so that equality holds. Denote this new set B, so $B' \subseteq B$ and $B = \sum_{i=1}^n |A_i| - n - \deg(f)$. Let $g \in F[x_1, \ldots, x_n]$ be the following polynomial

$$g(\mathbf{x}) = f(\mathbf{x}) \prod_{b \in B} \left(\sum_{i=1}^n x_i - b \right).$$

First, by adding degrees we see $\deg(g) = \deg(f) + |B|$, substituting the definition of B yields $\deg(g) = \sum_{i=1}^n |A_i| - n$. Moreover, for all $\mathbf{a} \in \prod_{i=1}^n A_i$ we have either $f(\mathbf{a}) = 0$ or $\mathbf{a} \in B' \subseteq B$. So, in either case

$$g(\mathbf{a}) = 0 \text{ for all } \mathbf{a} \in \prod_{i=1}^n A_i. \tag{3.2}$$

Then, observe that any maximal degree monomial in g will be the result of a maximal degree monomial of f, times $(\sum_{i=1}^n x_i)^{|B|}$, the maximal degree monomials in $\prod_{b \in B} (\sum_{i=1}^n x_i - b)$. Moreover,

$$\left[x_1^{|A_1|-1} \ldots x_n^{|A_n|-1} \right] g(\mathbf{x}) = \left[x_1^{|A_1|-1} \ldots x_n^{|A_n|-1} \right] f(\mathbf{x}) \cdot \left(\sum_{i=1}^n x_i \right)^{|B|}.$$

Applying the definition of B, we see this is precisely the same coefficient we assumed was nonzero in (3.1). So, $\left[x_1^{|A_1|-1} \ldots x_n^{|A_n|-1} \right] g(\mathbf{x}) \neq 0$. So, since $\deg(g) \leq \sum_{i=1}^n |A_i| - n$, we see equality holds, that is $\deg(g) = \sum_{i=1}^n (|A_i| - 1)$, so g satisfies the conditions for theorem 2.3, implying there is a $\mathbf{a} \in \prod_{i=1}^n A_i$ so that $g(\mathbf{a}) \neq 0$, a contradiction with (3.2). So, $B = \left| {}_f\bigoplus_{i=1}^n A_i \right| > \sum_{i=1}^n |A_i| - n - \deg(f)$. So, the lemma holds true. □

Theorem 3.3 (Erdős-Heilbronn Conjecture [1])**.** For a prime p and nonempty $A, B \subseteq C_p$, then $|A \oplus B| \geq \min\{p, |A| + |B| - \delta\}$ where $\delta = 3$ for the case $A = B$ and $\delta = 2$ in all other cases.

Proof. First of all, if without loss of generality $A = \{a\}$, then $A \oplus B = \{a + b : b \in B, a \neq b\}$, and since at most one $b = a$ we have $|A \oplus B| \geq |B| - 1 = |A| + |B| - 2$, so the claim holds.

So, we can assume $|A|, |B| \geq 2$. If $p = 2$, then $|A|, |B| = 2$, so $A = B = \{a_1, a_2\}$ and $|A| + |B| - 3 = 1$. Of course, by assumption $a_1 \neq a_2$, so $a_1 + a_2 \in A \oplus B$ proving the case for $p = 2$ since there is at least 1 element in the sumset. So, we can also assume $p \geq 3$.

If $|A| + |B| - 1 > p$, so $|A| + |B| \geq p + 2$, then Theorem 1.5 implies there are two representations $x_1 + y_1$ and $x_2 + y_2$ of every $x \in C_p$ with $x_1, y_1 \in A$, $x_2, y_2 \in B$. Suppose $x_1 = y_1$ and $x_2 = y_2$. Then we have $2x_1 = 2x_2 = x$. Since $p \geq 3$ is prime, hence odd, we see $2x_1 = 2x_2$ implies $x_1 = x_2$, a contradiction, so at least one representation will have two distinct elements, i.e., $x_1 \neq y_1$, so $x_1 + y_1 = x \in A \oplus B$. Since x was arbitrary in C_p, we see $|A \oplus B| = p \leq |A| + |B| - 1$, so this case holds as well. Thus, it remains only to show the case $|A| + |B| - 1 \leq p$.

Since $|A|, |B| \geq 2$, we must also have $|A|, |B| \leq p - 1$ else $|A| + |B| - 1 \leq p$ would be violated. Suppose $|A| \neq |B|$, then $A \oplus B = A \,{}_f\!\oplus B$ where $f = x - y \in C_p[x, y]$. Since $\deg(f) = 1 \leq |A| + |B| - 2$ by assumption, we need only show

$$\left[x^{|A|-1}y^{|B|-1}\right]\left(f(x,y)\cdot(x+y)^{|A|+|B|-3}\right) \neq 0 \tag{3.3}$$

in order to apply lemma 3.3 and obtain our result: $|A \oplus B| \geq |A| + |B| - 2$.

Substiting $(x - y)$ in place of f, we wish to examine $\left[x^{|A|-1}y^{|B|-1}\right](x - y)(x + y)^{|A|+|B|-3}$. Distributing, we see this is simply $\left[x^{|A|-2}y^{|B|-1}\right](x + y)^{|A|+|B|-3} - \left[x^{|A|-1}y^{|B|-2}\right](x + y)^{|A|+|B|-3}$. Next, applying Theorem

1.2, we see

$$\left[x^{|A|-1}y^{|B|-1}\right]\left(((x-y)\cdot(x+y)^{|A|+|B|-3}\right)=\binom{|A|+|B|-3}{|A|-2}-\binom{|A|+|B|-3}{|A|-1} \tag{3.4}$$

$$=(|A|-|B|)\,\frac{(|A|+|B|-3)\,(|A|+|B|-4)\ldots(|B|)}{(|A|-1)!}. \tag{3.5}$$

Since $|A|\neq|B|$ with both sets being of cardinality at most $p-1$, we have $|A|-|B|\not\equiv 0 \mod p$. Similarly, since $|A|+|B|-1\leq p$, we have all factors of the numerator in (3.5) being nonzero $\mod p$, so their product is nonzero $\mod p$. Thus, we see for $|A|\neq|B|$, we have

$$\left[x^{|A|-1}y^{|B|-1}\right]\left(f\,(x,y)\cdot(x+y)^{|A|+|B|-3}\right)\neq 0\in C_p.$$

Next, if $A=B$, then we may simply subtract one $b\in B$ to produce the set $B'=B\setminus\{b\}$ with $|B'|\neq|B|$, so the previous case implies the claim holds for $A\oplus B'$, so since $A\oplus B'\subseteq A\oplus B$, the claim holds for $A\oplus B$.

Finally, if $|A|=|B|$, but $A\neq B$ with $A\cap B=\varnothing$, then $A\oplus B=A+B$ and Theorem 3.1 proves the claim true. If $A\cap B\neq\varnothing$, then $A\cap B\neq A\cup B$ as $A\neq B$ and $|A\cap B|\neq|A\cup B|$, so we can apply the earlier case to find

$$|(A\cap B)\oplus(A\cup B)|\geq|A\cap B|+|A\cup B|-2=|A|+|B|-2. \tag{3.6}$$

Let $a+b\in(A\cap B)\oplus(A\cup B)$ and without loss of generality suppose $a\in A\cap B$ and $b\in A\cup B$. Then, if $b\in B$, we have $a\in A$ and $a\neq b$, so $a+b\in A\oplus B$. If $b\in A$, then $a\in B$, so $a+b\in A\oplus B$. So, $(A\cap B)\oplus(A\cup B)\subseteq A\oplus B$. Hence (3.6) implies $|A\oplus B|\geq|A|+|B|-2$, so the claim holds. Since the claim held for all possible $A,B\subseteq C_p$ this completes the proof. □

It is of note that in the last part of the proof, equality actually holds for the sumsets, that is

$$(A \cap B) \oplus (A \cup B) = A \oplus B.$$

This observation may be of use to the reader who chooses to study sumsets in further detail, but for this theorem inclusion, not equality, is all that was required.

A Nice Result for Graphs

Finally, to showcase the versatility of these tools we give two short results from graph theory, proved using the Combinatorial Nullstellensatz. For these proofs, graphs will be finite and will not contain loops.

Notation. We define the following standard graph objects. Let G be a graph. Then

- $E(G)$ is the set of all edges in G, and $e(G) \coloneqq |E(G)|$.
- $V(G)$ is the set of all vertices in G, and $v(G) \coloneqq |V(G)|$.
- For a $v \in V(G)$, $d(v)$ is the degree of v, or the number of edges it is part of.
- The incidence matrix of G has rows corresponding to vertices and columns corresponding to edges. An entry is 1 if its vertex is contained in its edge and it is 0 otherwise.
- A graph G is said to be p-regular if $d(v) = p$ for all $v \in V(G)$.
- $d(G) = \frac{1}{v(G)} \sum_{v \in V(G)} d(v)$ is the average degree over all $v \in V(G)$.

Lemma 3.4. Let G be a graph. Then, $\sum_{v \in V} d(v) = 2e(G)$. Consequently $d(G)\, v(G) = 2e(G)$

Proof. First, it is clear the claim holds if G contains only 1 edge. Now, we proceed by induction. If G contains k edges, we may remove one to induce the graph G', since the edge joined two vertices, we see we have removed 2 from the total degree. Hence, $\sum_{v \in V(G)} d(v) = \sum_{v \in V(G')} d(v) + 2 = 2e(G') + 2 = 2(e(G') + 1) = 2e(G)$ by applying the inductive hypothesis. So the claim is shown.

For the second claim, simply apply the definition of average degree. □

Theorem 3.4 ([1])**.** Let p be an odd prime and G a graph with $d(G) > 2p-2$ and maximum degree at most $2p-1$. Then there is a nontrivial p-regular subgraph.

Proof. Let $B = (b_{v,e})$ be the incidence matrix of G. For each $e \in E(G)$, let x_e be an associated variable taking on values 0 or 1 and define $F \in \mathbb{F}_p\left[(x_e)_{e(G)}\right]$ to be the polynomial

$$F((x_e)_{e\in E(G)}) = \prod_{v\in V}\left[1-\left(\sum_{e\in E} b_{v,e}x_e\right)^{p-1}\right] - \prod_{e\in E}(1-x_e). \tag{3.7}$$

The degree of the first product is $(p-1)v(G) = \frac{2p-2}{2}v(G) < \frac{1}{2}d(G)v(G) = e(G)$. The degree of the second product is clearly $e(G)$, simply taking the term consisting of the product over all x_e, $e \in E(G)$. So, $\deg(F) = |E|$. Then, since the coefficient of the maximum order term is nonzero with each x_e being to the first power, we can apply theorem 2.3 with each $A_i = \{0,1\}$ ($d_i = 1 < 2 = |A_i|$ clearly holds) to see there is a $(x_e)_{e\in E(G)} = \mathbf{x} \in \{0,1\}^{e(G)}$ such that $F(\mathbf{x}) \neq 0$, and as $F\left((0)_{e\in E(G)}\right) = 0$, we see $\mathbf{x} \neq (0)_{e\in E(G)}$.

Lastly, since the second term of (3.7) is clearly zero when evaluated at $\mathbf{x}$, we must have $\prod_{v\in V}\left[1-\left(\sum_{e\in E} b_{v;e}x_e\right)\right] = 1$. So, $\sum_{e\in E} b_{v;e}x_e = 0$ for every $v \in V(G)$.

So, letting H be the subgraph induced by $e(H) = \{e \in E(G) : x_e = 1\}$, we see every $v \in V(H)$ has $p \mid \sum_{e\in E(H)} b_{v;e}x_e$ (since we are working mod p) and, since the maximum degree was at most $2p-2$ and H cannot contain isolated points (since it was generated by edges), we must have $p = \sum_{e\in E} b_{v;e}x_e$. Since $x_e = 1$ for all $e \in E(H)$, we see $\sum_{e\in E} b_{b;e}x_e = d_H(v)$ where d_H is the degree in H. So, H is p-regular. □

Chapter 4

Zeilberger-Bressoud q-Dyson Theorem

The previous results have all been relatively simple applications of the Combinatorial Nullstellensatz. Now, we show its use in a more complex proof. We will construct a generalized laurent polynomial based on the g and prove the exact value of its constant term. To begin, we define a new operation, the q-falling factorial and draw an analog to the traditional

Definition 4.1 (q-Falling factorial)**.** For a ring R, a $q \in R$, and a $k \in \mathbb{N}_0$ we define

$$(x)_{k;q} = (1-x)(1-xq)\left(1-xq^2\right)\ldots\left(1-xq^{k-1}\right).$$

For convenience $(x)_{0;q} \coloneqq 1$.

As it is unnecessary in the following proofs, we will omit the q from notation so that $(x)_{k;q} = (x)_k$ for an assumed independent variable q.

For simplicity, when referring to this object we will call it the **q-falling factorial**, though this covention is not found in the literature and is simply adopted for convenience.

The Dyson Conjecture and Lagrange Interpolation

In pursuit of a proof in statistical physics, Dyson himself originally made the following conjecture in 1963, [9].

Theorem 4.1 (Dyson's Conjecture)**.** Let $a_1, \ldots, a_n \in \mathbb{N}_0$. Then,

$$[x_1^0 \ldots x_n^0] \left(\prod_{1 \leq i < j \leq n} \left(1 - \frac{x_i}{x_j}\right)^{a_i} \right) = \frac{(\sum_{i=1}^n a_i)!}{\prod_{i=1}^n (a_i!)}.$$

Many proofs were later discovered of this theorem buy Gunson (a result which remained unpublished), Wilson [14], and Good [6]. Good's proof using univariate Lagrange interpolation was remarkably simple.

Lagrange interpolation, of course, is another fundamental tool of the polynomial method. In this thesis we do not prove it (as it is a standard result of calculus) but we will state the following multivariate form:

Theorem 4.2 (Multivariate Lagrange Interpolation)**.** Let $A_1, \ldots, A_n \subseteq \mathbb{F}$, a field. Then a laurent polynomial $F(\mathbf{x})$ in n variables with $\deg(F) > \sum_{i=1}^n |A_i|$ has a unique interpolation polynomial of the form

$$\widetilde{F}(\mathbf{x}) = \sum_{\mathbf{c} \in \prod_{i=1}^n A_i} F(\mathbf{c}) \prod_{i=1}^n \prod_{\gamma \in A_i \setminus \{c_i\}} \frac{x_i - \gamma}{c_i - \gamma}$$

for $\mathbf{c} = (c_1, \ldots, c_n)$.

This is a slightly weaker variation of the theorem presented in [12] (in fact less points are required to guarantee interpolation).

The q-Dyson Theorem

A direct generalization of this, the Zeilberger-Bressoud q-Dyson theorem was originally posed by Andrews in 1975 [4] and this proof using lagrangian interpolation was published by Károlyi and Nagy.

Theorem 4.3 (q-Dyson Theorem[8])**.** First, let $a_1, \ldots, a_n \in \mathbb{N}_0$. Then define the following polynomial:

$$f_q(\mathbf{x}) = f_q(x_1, x_2, \ldots, x_n) \coloneqq \prod_{1 \le i < j \le n} \left(\frac{x_i}{x_j}\right)_{a_i} \left(\frac{qx_j}{x_i}\right)_{a_j}.$$

Then,

$$[x_1^0 \ldots x_n^0] f_q(\mathbf{x}) = \frac{(q)_{\sum_{i=1}^n a_i}}{\prod_{j=1}^n (q)_{a_j}}.$$

Before we can prove this result, we must examine a related function and prove a result about its coefficients. Note that this lemma makes implicit use of the Combinatorial Nullstellenstatz when using lagrangian interpolation.

Lemma 4.1. Let $\mathbb{F}$ be a field and $F \in \mathbb{F}[x_1, \ldots, x_n]$ to be a polynomial of degree $d \le \sum_{i=1}^n d_i$. Let $A_1, \ldots, A_n \subseteq \mathbb{F}$ be subsets with $|A_i| = d_i + 1$ for each $1 \le i \le n$, then

$$\left[\prod_{i=1}^n x_i^{d_i}\right] F = \sum_{c_1 \in A_1, c_2 \in A_2, \ldots, c_n \in A_n} \frac{F(c_1, c_2, \ldots, c_n)}{\varphi_1'(c_1)\varphi_2'(c_2)\ldots\varphi_n'(c_n)}$$

with $\varphi_i(z) = \prod_{a \in A_i}(z - a)$ and φ_i' being its derivative.

Proof. We construct a sequence of polynomials. Let $F_0 = F$ and define F_i as follows. Let $F_i(\mathbf{x}) = \frac{F_{i-1}}{\varphi_i(x_i)}$ as a laurent polynomial in n variables. We see this construction guarantees $\left[\prod_{i=1}^n x_i^{d_i}\right] F_{i-1} = \left[\prod_{i=1}^n x_i^{d_i}\right] F_i$ and for all $\mathbf{c} \in \prod_{i=1}^n A_i$ we see $F_n(\mathbf{c}) = F(\mathbf{c})$ and $\deg_{x_i}(F_i) \le d_i$ for all $1 \le i \le n$, hence as $\sum_{i=1}^n |A_i| > \deg(F)$, we see lagrangian

interpolation yields a unique polynomial

$$\widetilde{F}_n(\mathbf{x}) = \sum_{\mathbf{c}\in\prod_{i=1}^n A_i} F(\mathbf{c}) \prod_{i=1}^n \prod_{\gamma\in A_i\setminus c_i} \frac{x_i-\gamma}{c_i-\gamma}.$$

so that $\widetilde{F}_n(\mathbf{x}) = F_n(\mathbf{x})$ for all $\mathbf{x}\in\mathbb{F}^n$. Given $\varphi_i(z) = \prod_{a\in A_i}(z-a)$, we have $\varphi_i'(z) = \sum_{a_k\in A_i}\prod_{i=a\in A_i\setminus a_k}(z-a)$, and evaluating at a $c_i\in A_i$ yields $\varphi_i'(c_i) = \prod_{a\in A_i\setminus c_i}(c_i-a)$. We note that $\left[\prod_{i=1}^n x_i^{d_i}\right] F_n(\mathbf{x}) = \sum_{c\in\prod_{i=1}^n A_i} \frac{F(\mathbf{c})}{\prod_{i=1}^n\prod_{\gamma\in A_i\setminus c_i}(c_i-\gamma)} = \frac{F(\mathbf{c})}{\prod_{i=1}^n\varphi_i'(c_i)}$. This completes the lemma. □

Now, we prove theorem 4.3.

Proof of theorem 4.3. First, we note that if $a_i = 0$, then $(x)_{a_i} = (1-x)$, hence we may omit all of these terms as they will not affect the constant. Hence, we know each (relevant) a_i is a positive integer. Let

$$F(\mathbf{x}) = \prod_{1\le i<j\le n}\left(\prod_{i=0}^{a_i-1}(x_j - x_i q^t)\cdot\prod_{t=1}^{a_j}(x_i - x_j q^t)\right).$$

Denote $\kappa = \frac{1}{\prod_{1\leq i<j\leq n} x_i^{a_j} x_j^{a_i}}$. Then, we see

$$\begin{aligned}
f_q(x_1, x_2, \ldots, x_n) &= \prod_{1\leq i<j\leq n} [\prod_{k=1}^{a_i} \left(1 - \frac{x_i}{x_j} q^{k-1}\right) \prod_{k=1}^{a_j} \left(1 - \frac{x_j}{x_i} q^k\right)] \\
&= \prod_{1\leq i<j\leq n} \frac{1}{x_j^{a_i} x_i^{a_j}} [\prod_{k=1}^{a_i} \left(x_j - x_i q^{k-1}\right) \prod_{i=1}^{a_j} \left(x_i - x_j q^k\right)] \\
&= \frac{1}{\prod_{1\leq i<j\leq n} x_i^{a_j} x_j^{a_i}} \underbrace{\prod_{1\leq i<j\leq n} [\prod_{k=1}^{a_i} \left(x_j - x_i q^{k-1}\right) \prod_{k=1}^{a_j} \left(x_i - x_j q^k\right)]}_{=F(x_1, x_2, \ldots, x_n)} \\
&= \kappa \prod_{1\leq i<j\leq n} \left(x_j^{a_i} + \beta_i\right) \left(x_i^{a_j} + \beta_j\right) \\
&= \kappa \prod_{1\leq i<j\leq n} \left(x_j^{a_i} x_i^{a_j} + \beta_{ij}\right) \\
&= c\kappa \left(\prod_{1\leq i<j\leq n} x_j^{a_i} x_i^{a_j}\right) + \beta,
\end{aligned}$$

where $\beta_i, \beta_j, \beta_{ij}, \beta$ are all of the lower order terms from their respective product. We see the first term is simply a constant, and we see as the exponent of x_i will take on all values, a_k, except a_i and similarly, the exponent of x_j will take on all values except a_j. Hence, we find [1] $f_q(\mathbf{x}) = \left[\prod_{i=1}^n x_i^{\sum_{k=1}^n a_k - a_i}\right] F(\mathbf{x})$.

Now, we define $\sum_{i=1}^n a_i = \sigma$, $A_i = \{1, q, \ldots, q^{\sigma - a_i}\}$ and a sequence $\sigma_0 = 0$, $\sigma_i = \sum_{j=1}^{i-1} a_j$ for $2 \leq i \leq n+1$. It is clear $|A_i| = \sigma - a_i + 1$ and $\sigma_{n+1} = \sigma$. Now, we aim to prove that for $\mathbf{c} = (c_1, \ldots, c_n) \in \prod_{i=1}^n A_i$, we have $F(\mathbf{c}) = 0$ unless $c_i = q^{\sigma_i}$ for each $1 \leq i \leq n$.

We will suppose a contradiction, that is there exists a $(c_1, c_2, \ldots, c_n) = \mathbf{c} \in \prod_{i=1}^n A_i$ such that $F(\mathbf{c}) \neq 0$ for $c_i = q^{\alpha_i}$ where $0 \leq \alpha_i \leq \sigma - a_i$. Then, we see for a pair $j > i$, we have $\alpha_j - \alpha_i \geq a_i$, in particular every pair α_j, α_i with $i \neq j$ is distinct. Then, we see their is a unique ordering π such that $\alpha_{\pi(1)} < \alpha_{\pi(2)} < \ldots < \alpha_{\pi(n)}$. Then, summing over the inequality $\alpha_{\pi(i+1)} - \alpha_{\pi(i)} \geq a_{\pi(i)}$

for $1 \leq i \leq n-1$ yields

$$\begin{aligned}\left(\alpha_{\pi(_n)} - \alpha_{\pi(n-1)}\right) + \left(\alpha_{\pi(n-1)} - \alpha_{\pi(n-2)}\right) + \ldots + \left(\alpha_{\pi(2)} - \alpha_{\pi(1)}\right) &= \alpha_{\pi(n)} - \alpha_{\pi(1)} \\ &\geq \sum_{i=1}^{n-1} a_{\pi(i)} \\ &= \sigma - a_{\pi(n)}.\end{aligned}$$

Then, as $\alpha_{\pi(1)} \geq 0$ and $\alpha_{\pi(n)} \leq \sigma - a_{\pi(n)}$ by the original inequality, we find equality must hold, hence

$$\alpha_{\pi(n)} - \alpha_{\pi(1)} = \sigma - a_{\pi(n)} = \sigma_n.$$

We see this summation works over $k < n-1$ terms as well, so $\alpha_{\pi(k)} = \sigma_k$ hence π must be the identity permutation and we see $\alpha_k = \sum_{i=1}^{k-1} a_i = \sigma_k$ for all $1 \leq k \leq n$. $\lightning$. Hence, we see $F(\mathbf{c}) = 0$ unless each $c_i = q^{\sigma_i}$, so the constant

$$[1]\, f_q = \frac{F\left(q^{\sigma_1}, \ldots, q^{\sigma_n}\right)}{\varphi_1'\left(q^{\sigma_1}\right) \ldots \varphi_n'\left(q^{\sigma_n}\right)}$$

by the lemma.

Now, denote $\tau_i = \binom{\sigma_i}{2} + \sigma_i\left(\sigma - \sigma_i + 1\right)$ and we derive a q-falling factorial form of $\varphi_i'\left(q^{\sigma_i}\right)$.

Then we see

$$
\begin{aligned}
\varphi_i'\left(q^{\sigma_i}\right) &= \prod_{\substack{0\le t\le \sigma-a_i \\ t\neq\sigma_i}} \left(q^{\sigma_i}-q^t\right) \\
&= \prod_{t=0}^{\sigma_i-1}\left(q^{\sigma_i}-q^t\right)\prod_{t=\sigma_i+1}^{\sigma-a_i}\left(q^{\sigma_i}-q^t\right) \\
&= \prod_{t=0}^{\sigma_i-1}(-q)^t\left(1-q^{\sigma_i-t}\right)\prod_{t=1}^{\sigma-\sigma_i-a_i} q^{\sigma_i}\left(1-q^t\right) \\
&= (-1)^{\sigma_i}\cdot \underbrace{\prod_{i=1}^{\sigma_i-1} q^t}_{=q^{\sum_{i=1}^{\sigma_i-1}1}=q^{\frac{\sigma_i(\sigma_i-1)}{2}}=q^{\binom{\sigma_i}{2}}} \cdot \underbrace{\prod_{i=0}^{\sigma_i-1}(1-q^{\sigma_i-t})}_{=(q)_{\sigma_i}} \cdot \underbrace{\prod_{i=1}^{\sigma-\sigma_{i+1}} q^{\sigma_i}}_{=q^{\sigma_i(\sigma-\sigma_{i+1})}} \cdot \underbrace{\prod_{i=1}^{\sigma-\sigma_{i+1}}\left(1-q^t\right)}_{=(q)_{\sigma-\sigma_{i+1}}} \\
&= (-1)^{\sigma_i} q^{\binom{\sigma_i}{2}+\sigma_i(\sigma-\sigma_{i+1})}(q)_{\sigma_i}(q)_{\sigma-\sigma_{i+1}} \\
&= (-1)^{\sigma_i} q^{\tau_i}(q)_{\sigma_i}(q)_{\sigma-\sigma_{i+1}}.
\end{aligned}
$$

Similarly by double counting the terms and performing simple manipulations, we find $F\left(q^{\sigma_1},\ldots,q^{\sigma_n}\right)$ in a g form. First, note that we can write a partial sequence from $(\sigma_j-\sigma_i-a_i)=(\sigma_j-\sigma_{i+1})$ to $(\sigma_j-\sigma_i)$ as

$$
\prod_{t=0}^{a_i-1}\left(1-q^{\sigma_j-\sigma_i-t}\right)=\frac{\prod_{t=1}^{\sigma_j-\sigma_i}(1-q^t)}{\prod_{t=1}^{\sigma_j-\sigma_i-a_i}(1-q^t)}=\frac{\prod_{t=1}^{\sigma_j-\sigma_i}(1-q^t)}{\prod_{t=1}^{\sigma_j-\sigma_{i+1}}(1-q^t)}=\frac{(q)_{\sigma_j-\sigma_i}}{(q)_{\sigma_j-\sigma_{i+1}}}.
$$

Similarly, we find a partial sequence from $(\sigma_j-\sigma_i)$ to $(\sigma_j+a_j-\sigma_i)=(\sigma_{j+1}-\sigma_i)$ to be

$$
\prod_{t=1}^{a_j}\left(1-q^{\sigma_j-\sigma_i+t}\right)=\frac{\prod_{t=1}^{\sigma_j+a_j-\sigma_i}(1-q^t)}{\prod_{t=1}^{\sigma_j-\sigma_i}(1-q^t)}=\frac{\prod_{t=1}^{\sigma_{j+1}-\sigma_i}(1-q^t)}{\prod_{t=1}^{\sigma_j-\sigma_i}(1-q^t)}=\frac{(q)_{\sigma_{j+1}-\sigma_i}}{(q)_{\sigma_j-\sigma_i}}.
$$

Now, let $u=\sum_{i=1}^{n}(n-i)\,a_i$ and $v=\sum_{i=1}^{n}\left[(n-i)\left(a_i+\sigma_i+\binom{a_i}{2}\right)+\sigma_i\left(\sigma-\sigma_{i+1}\right)\right]$

and we see

$$
\begin{aligned}
F\left(q^{\sigma_1}, q^{\sigma_2}, \ldots, q^{\sigma_n}\right) &= \prod_{1\le i<j\le n} \left(\prod_{t=0}^{a_i-1} \left(q^{\sigma_j} - q^{\sigma_i} q^t\right) \cdot \prod_{t=1}^{a_j} \left(q^{\sigma_i} - q^{\sigma_j} q^t\right) \right) \\
&= \prod_{1\le i<j\le n} (-1)^{a_i} \left(\underbrace{\prod_{t=0}^{a_i-1} q^{\sigma_i+t}}_{=q^{a_i\sigma_i} q^{\binom{a_i}{2}}} \underbrace{\prod_{t=0}^{a_i-1} (1-q^{\sigma_j-\sigma_i-t})}_{=\frac{(q)_{\sigma_j-\sigma_i}}{(q)_{\sigma_j-\sigma_{i+1}}}} \cdot \underbrace{\prod_{t=1}^{a_j} q^{\sigma_i}}_{=q^{\sigma_i(\sigma-\sigma_{i+1})}} \underbrace{\prod_{t=1}^{a_j} \left(1-q^{\sigma_j-\sigma_i+t}\right)}_{=\frac{(q)_{\sigma_{j+1}-\sigma_i}}{(q)_{\sigma_j-\sigma_i}}} \right) \\
&= (-1)^{\sum_{i=1}^n (n-i)a_i} \, q^{\sum_{i=1}^n \left[(n-i)(a_i\sigma_i+\binom{a_i}{2})+\sigma_i(\sigma-\sigma_{i+1})\right]} \prod_{1\le i<j\le n} \frac{(q)_{\sigma_{j+1}-\sigma_i}}{(q)_{\sigma_j-\sigma_{i+1}}} \\
&= (-1)^u \, q^v \frac{\prod_{i=1}^{n-1} \prod_{j=i+1}^{n} (q)_{\sigma_{j+1}-\sigma_i}}{\prod_{i=1}^{n-1} \prod_{j=i+1}^{n} (q)_{\sigma_j-\sigma_{i+1}}} \\
&= (-1)^u \, q^v \frac{\prod_{i=1}^{n-1} \prod_{j=i+2}^{n+1} (q)_{\sigma_j-\sigma_i}}{\prod_{i=2}^{n} \prod_{j=i}^{n} (q)_{\sigma_j-\sigma_i}} \\
&= (-1)^u \, q^v \frac{\prod_{j=3}^{n+1} (q)_{\sigma_j-\sigma_1} (\prod_{i=2}^{n-1} \prod_{j=i+2}^{n} (q)_{\sigma_j-\sigma_i})(\prod_{i=2}^{n-1} (q)_{\sigma_{n+1}-\sigma_i})}{(\prod_{i=2}^{n-1} \prod_{j=i+2}^{n} (q)_{\sigma_j-\sigma_i})(\prod_{i=2}^{n-1} \prod_{j=i}^{i+1} (q)_{\sigma_j-\sigma_i})} \\
&= (-1)^u \, q^v \frac{\prod_{i=2}^{n-1} (q)_{\sigma-\sigma_i} \prod_{j=3}^{n+1} (q)_{\sigma_j-\sigma_1}}{\prod_{i=2}^{n-1} (q)_{\sigma_{i+1}-\sigma_i}} \cdot \frac{(q)_{\sigma_2-\sigma_1}}{(q)_{\sigma_2-\sigma_1}} \cdot \frac{(q)_{\sigma-\sigma_n}}{(q)_{\sigma-\sigma_n}} \underbrace{(q)_{\sigma_1-\sigma_1}}_{1} \\
&= (-1)^u \, q^v \frac{\prod_{i=2}^{n} (q)_{\sigma-\sigma_i} \cdot (q)_{\sigma-\sigma_1} \cdot \prod_{i=1}^{n} (q)_{\sigma_i}}{\prod_{i=1}^{n} (q)_{\sigma_{i+1}-\sigma_i}} \\
&= (-1)^u \, q^v \prod_{i=1}^{n} \frac{(q)_{\sigma_i} (q)_{\sigma-\sigma_i}}{(q)_{\sigma_{i+1}-\sigma_i}}.
\end{aligned}
$$

From here, we see

$$\begin{aligned}\sum_{i=1}^{n}(n-i)\,a_i &= (n-1)\,a_1+(n-2)\,a_2+\ldots+0a_n\\ &= \sum_{i=1}^{n-1}a_i+\sum_{i=1}^{n-2}a_i+\ldots+\sum_{i=1}^{1}a_i+\underbrace{\sum_{i=1}^{0}a_i}_{0}\\ &= \sigma_n+\sigma_{n-1}+\ldots+\sigma_2+\underbrace{\sigma_1}_{0}\\ &= \sum_{i=1}^{n}\sigma_i.\end{aligned}$$

Hence, $u=\sum_{i=1}^{n}\sigma_i$ and the powers of -1 will vanish. Moreover, we show by induction that the powers of q vanish, that is $\sum_{i=1}^{n}(n-i)\left(a_i\sigma_i+\binom{a_i}{2}\right)=\sum_{i=1}^{n}\binom{\sigma_i}{2}$. Note that for $j=0$, we have $\sum_{i=1}^{0}(0-i)\left(a_i\sigma_i+\binom{a_i}{2}\right)=\sum_{i=1}^{0}\binom{\sigma_i}{2}=0$. Similarly, the case $n=1$ holds. Then, for the general case, we simply expand the right hand side as follows:

$$\sum_{i=2}^{n}\binom{\sigma_i}{2}=\binom{\sigma_2}{2}+\ldots+\binom{\sigma_n}{2} \tag{4.1}$$

$$=\frac{1}{2}\Bigg[(a_1-1)\,a_1+(a_1+a_2-1)\,(a_1+a_2)+\ldots \tag{4.2}$$

$$+(a_1+\ldots+a_{n-1}-1)\,(a_1+\ldots+a_{n-1})\Bigg]. \tag{4.3}$$

First, grouping the squares and the terms involving -1 and then grouping the remaining products yields

$$\begin{aligned}
&(a_1 + \ldots + a_{n-1} - 1)(a_1 + \ldots + a_{n-1}) \\
&\qquad = a_{n-1}^2 - a_{n-1} + a_{n-2}^2 - a_{n-2} + \ldots + a_1^2 - a_1 + \\
&\qquad\quad + a_{n-1}(a_1 + \ldots + a_{n-2}) + a_{n-2}(a_1 + \ldots + a_{n-3}) + a_{n-2}a_{n-1} \\
&\qquad\quad + a_{n-3}(a_1 + \ldots + a_{n-4}) + a_{n-3}(a_{n-2} + a_{n-1}) + \ldots \\
&\qquad\quad + a_3(a_1 + a_2) + a_3(a_4 + \ldots + a_{n-1}) + a_2a_1 + a_2(a_3 + \ldots + a_{n-1}) \\
&\qquad\quad + a_1(a_2 + \ldots + a_{n-1}).
\end{aligned}$$

Collecting terms yields

$$= (a_{n-1} - 1)a_{n-1} + \ldots + (a_1 - 1)a_1 + 2a_{n-1}\sigma_{n-1} + \ldots + 2a_2\sigma_2.$$

Applying this identity to (4.3) and adding zero terms where necessary gives the result:

$$\begin{aligned}
\sum_{i=2}^{n} \binom{\sigma_i}{2} &= a_{n-1}\sigma_{n-1} + \binom{a_{n-1}}{2} + 2\left(a_{n-2}\sigma_{n-2} + \binom{a_{n-2}}{2}\right) \\
&\qquad + \ldots + (n-2)\left(a_2\sigma_2 + \binom{a_2}{2}\right) \\
&= \sum_{i=1}^{n-i} (n-i)\left(a_i\sigma_i + \binom{a_i}{2}\right).
\end{aligned}$$

Assembling all results yields

$$
\begin{aligned}
[1]\, f_q(\mathbf{x}) = \frac{F\left(q^{\sigma_1},\ldots,q^{\sigma_n}\right)}{\varphi_1'\left(q^{\sigma_1}\right)\ldots\varphi_n'\left(q^{\sigma_n}\right)} &= \prod_{i=1}^{n} \frac{(q)_{\sigma_i}(q)_{\sigma-\sigma_i}}{(q)_{\sigma_i}(q)_{\sigma-\sigma_{i+1}}(q)_{\sigma_{i+1}-\sigma_i}} \\
&= \frac{(q)_{\sigma-\sigma_1}}{\prod_{i=1}^{n}(q)_{\sigma_{i+1}-\sigma_i}} \\
&= \frac{(q)_{\sigma}}{\prod_{i=1}^{n}(q)_{a_i}} \\
&= \frac{(q)_{a_1+a_2+\ldots+a_n}}{(q)_{a_1}\ldots(q)_{a_n}}.
\end{aligned}
$$

□

Chapter 5

Zero-Sum Theory

Definitions and Notation

As its name would imply, zero-sum theory is a branch of combinatorial number theory aiming to categorize exactly when a sequence contains a subsequence which sums to zero (mod some p). First, though, we must define a sequence and give a few basic results,

Definition 5.1. For an alphabet A (an arbitrary set of symbols), we define a **sequence** to be the string formed by the finite formal commutative multiplication of elements $a \in A$. That is, if S is a sequence in A, then $S = a_1 \cdot a_2 \cdot \ldots \cdot a_n = \prod_{i=1}^{n} a_i$ for some $a_i \in A$ where the a_i need not be distinct for different i. For the alphabet $\mathbb{Z}$, $S_0 = 1 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 4 = 4 \cdot 3 \cdot 2 \cdot 3 \cdot 1 \cdot 3$ is a sequence of length 6.

Since the multiplication is commutative, we generally fix an indexing of the sets where all duplicate terms have adjacent indices. Under this convention, we then will denote repeated terms by superscript, i.e. if $S = s_1 \cdot \ldots \cdot s_n$ and $s_i = s_{i+1}$, then we may instead write $S = s_1 \cdot \ldots \cdot s_i^2 \cdot s_{i+2} \cdot \ldots \cdot s_n$. This of course can be repeated to produce larger superscripts. For example, the sum S_0 from the previous example is equal to $1 \cdot 2 \cdot 3^3 \cdot 4$ under this notation.

For a sequence S we denote $|S|$ to be the length of S.

For a sequence $S = \prod_{i=1}^{n} s_i$ and an indexing set $I \subseteq [1, n]$ we let $S(I) = \prod_{i \in I} s_i$ be the **subsequence** indexed by I. If T is a subsequence of S, we write $T \mid S$.

For a sequence $S = \prod_{i=1}^{n} s_i$ and an indexed set $I \subseteq [1, n]$ let $S(I) = T$. Then, we denote the sequence $S([1, n] \setminus I) = ST^{-1}$. This sequence contains all the terms which were in S, but not T. For an abelian group $(G, +)$, we say a sequence $S = \prod_{i=1}^{n} s_i$ in G is **zero-sum** if $\sum_{i=1}^{n} s_i = 0_G$. Instead of writing $\sum_{i=1}^{n} s_i$, we often denote the sum over S to be $\sigma(S)$, so S is zero sum if $\sigma(S) = 0$.

There are alternative formulations of all of the following theorems using multi-sets, free abelian monoids, or other algebraic objects which encode the same behavior, but the sequence approach is the most standard.

Next, we define a few terms relating to abelian groups.

Definition 5.2. Recall a finite abelian group G has a unique decomposition into cyclic groups $G = C_{q_1} \oplus C_{q_2} \oplus \ldots \oplus C_{q_r}$. where $1 < q_1 < \ldots < q_r$ and $q_1 \mid q_2 \mid \ldots \mid q_r$. In this case, we of course know $|G| = \prod_{i=1}^{r} q_i$.
We define $\mathrm{Rank}\,(G) = r$ and $\exp(G) = q_r$ to be the **rank** and **exponent** of the group respectively. These two constants, as well as $|G|$, give three different notions of the size of a group.

As it turns out, most theorems in zero-sum theory will be concerned with the exponent of the abelian group G. As we alluded to earlier, our primary interest with sequences is when they contain subsequences which are zero-sum.

Definition 5.3. Let G be an abelian group, let S be a sequence in G, and let $p, q \in \mathbb{N}$. We define the following constants:

- $N_p(S)$ is the number of subsequences, $T \mid S$, where $|T| = p$ and $\sigma(T) = 0$.
- Similarly, $N_{p,q}(S)$ is the number of pairs of disjoint subsequences $T_1, T_2 \mid S$, where $|T_1| = p$, $|T_2| = q$, and $\sigma(T_1) = \sigma(T_2) = 0$.
- Let $T_1 \mid S$ be an arbitrary subsequence with $|T_1| = q$ and $\sigma(T_1) = 0$. Then, $N_p^q(S)$ is the subsequences $T_2 \mid T_1$ where $|T_2| = p$ and $\sigma(T_2) = 0$.
- $\mathsf{D}(G)$ is the minimal number such that any sequence, S in G, of length atleast $\mathsf{D}(G)$ will contain a nonempty zero-sum subsequence. We call this the **Davenport constant** for the group G.
- $\eta(G)$ is the minimal number such that any sequence S in G with $|S| \geq \eta(G)$ will contain a nonempty susbequence $T \mid S$ with $|T| \leq \exp(G)$ and $\sigma(T) = 0$. We sometimes call such zero-sum subsequences T with $|T| \leq \exp(G)$ **short zero-sum subsequences**.
- $\mathsf{s}\left(C_p^k\right)$ is the minimal number such that any sequence, S in $G = C_p^k$ with $|S| \geq \mathsf{s}\left(C_p^k\right)$ will contain a subsequence $T \mid S$ with $|T| = p = \exp(G)$ and $\sigma(T) = 0$.
- $\mathsf{s}_n\left(C_p^k\right)$ is the number such that any sequence S in $G = C_{p^k}$ with $|S| \geq \mathsf{s}_n\left(C_p^k\right)$ will contain a subsequence $T \mid S$ with $|T| = n$ and $\sigma(T) = 0$.
- If $G = C_{q_1} \oplus \ldots \oplus C_{q_r}$, then $\mathsf{D}^*(G) = 1 + \sum_{i=1}^{r}(q_i - 1)$.

Basic Proofs and Prerequisites

With these definitions out of the way, we now prove a few simple theorems concerning zero-sum sequences before showcasing two larger results. First, it is quite trivial to prove a loose upper bound on $\mathsf{D}(G)$, namely the order of G itself.

Proposition 5.1. Let G be a finite abelian group. Then, $\mathsf{D}(G) \leq |G|$.

Proof. Let $S = s_1 \dots s_n$ be a sequence in G with $|S| \geq |G|$. Let $S_k = \prod_{i=1}^{k} s_i$ for each $k \in [1, n]$, so $S_n = S$ and $S_1 = s_1$. Then, if $\sigma(S_k) = 0$ for some k, we are done. Otherwise, the pigeonhole principle proves there are two indices, $n_1 < n_2$ so that $\sigma(S_{n_1}) = \sigma(S_{n_2})$ since there are only $|G| - 1$ nonzero terms in G but at least $|G|$ subsequences S_k . Then, $T = \prod_{i=1+n_1}^{n_2} s_i$ has $\sigma(T) = \sigma(S_{n_2}) - \sigma(S_{n_1}) = 0$, so T is zero-sum and the claim is shown. □

It is also quite easy to prove that $\mathsf{D}^*(G)$ is a lower bound.

Proposition 5.2. Let G be a finite abelian group. Then, $\mathsf{D}(G) \geq \mathsf{D}^*(G)$.

Proof. Suppose $G = \bigoplus_{i=1}^{r} C_{q_i}$, with e_i being a generator for each C_{q_i}. Then $T = \prod_{i=1}^{r} e_i^{q_i - 1}$ is a sequence of length $\sum_{i=1}^{r} q_i - 1$ with no nontrivial zero-sum subsequences. To see this, note that a subsequence can only be zero-sum if each of its coordinates within the direct sum is zero-sum. Since $\operatorname{ord}(e_i) = q_i$, this cannot happen, so T can have no nontrivial zero-sum subsequences. Since $|T| + 1 = \mathsf{D}^*(G)$, we see $\mathsf{D}(G)$ is at least $\mathsf{D}^*(G)$, so the claim is shown. □

These two propositions of course imply $\mathsf{D}(C_p) = p$. The next chapter will generalize this notion to arbitrary p-groups.

There is one more theorem in basic zero-sum theory which we will not prove, but is deserving of mention, the davenport constant of a rank 2 abelian group.

Theorem 5.1. Let G be a finite abelian group of rank 2, that is $G = C_{n_1} \oplus C_{n_2}$ with $n_1 \mid n_2$. Then, $\mathsf{D}(G) = \mathsf{D}^*(G)$.

The proof of this theorem is relatively elementary, though it does require some homological algebra, so for this reason we exclude it from the current survey.

Finally, we provide proofs of the multiplicity of η, D, and s,

Theorem 5.2. Let $m, n \in \mathbb{N}$ and suppose it is already known that $\eta\left(C_n^2\right) = 3n-2$ and $\eta\left(C_m^2\right) = 3m-2$. Then $\eta\left(C_{nm}^2\right) = 3nm-2$.

Note that it suffices only to prove this is an upper bound as a counterexample of length $3mn-3$ is easily produced.

Proof. First, let $G = C_{mn}^2$ and note that $3mn-2 = m\left(3n-3\right)+3m-2$. Let $\varphi : C_{mn}^2 \to C_m^2,\ x \mapsto \varphi(x) = nx$ be the left multiplication by n map. Now, let $S = \prod_{i=1}^{3mn-2} g_i$ be a sequence in G of length $3mn-2$. Define $\varphi\left(S\right) \coloneqq \prod_{i=1}^{3mn-2} \varphi\left(g_i\right) = \prod_{i=1}^{3mn-2} ng_i \in C_m^2$. Since $\varphi\left(S\right)$ is a sequence in C_m^2 of length greater than $3m-2 = \eta\left(C_m^2\right)$, we find a zero-sum sequence $T_1 \mid \varphi\left(S\right)$ with $\left|T_1\right| \leq \exp\left(C_m^2\right) = m$. So, $\left|\varphi\left(S\right)T_1^{-1}\right| \geq 3mn-2-m = m\left(3n-2\right)+3m-2$. We repeat this process inductively, assuming we have found a subsequence $T_k \mid \varphi\left(S\right)T_1^{-1}T_2^{-1}\ldots T_{k-1}^{-1}$ with $\left|\varphi\left(S\right)T_1^{-1}\ldots T_k^{-1}\right| \geq m\left(3n-3-k\right)+3m-2 \geq \eta\left(C_m^2\right)$ we find another zero-sum subsequence $T_{k+1} \mid \varphi\left(S\right)T_1^{-1}\ldots T_k^{-1}$ with $\left|\varphi\left(S\right)T_1^{-1}\ldots T_{k+1}^{-1}\right| \geq m\left(3n-3-k-1\right)+3m-2$ for $1 \leq k \leq 3n-4$. So, in total we find $3n-3$ disjoint zero-sum subsequences $T_1\ldots T_{3n-3} \mid \varphi\left(S\right)$. Finally, since $\left|\varphi\left(S\right)T_1^{-1}\ldots T_{3n-3}^{-1}\right| \geq 3m-2$, we find one more zero-sum subsequence $T_{3n-2} \mid ST_1^{-1}\ldots T_{3n-3}^{-1}$

Now, note that $T_i = \prod_{j=1}^{\ell_i} ng_i^{(j)}$ where each $\ell_i \leq m$ and $g_i^{(j)} \mid S$, $1 \leq j \leq \ell_i$, is a unique element in S for each $1 \leq i \leq 3n-2$ (because the T_i were disjoint). Then, note that each $\sigma(\varphi^{-1}\left(T_i\right)) = \alpha_i m$ for some $\alpha_i \in C_n^2$. So, we can associate each $\sigma\left(\varphi^{-1}\left(T_i\right)\right)$ with an element $\alpha_i \in C_n^2$. Then,

$$X = \alpha_1 \ldots \alpha_{3n-2}$$

is a sequence in C_n^2 with $|X| = 3n-2 > \eta\left(C_n^2\right)$ so we find a $I \subseteq [1, 3n-2]$ with $|I| \leq n$ and $\sigma\left(X\left(I\right)\right) = 0$. So finally we see

$$Y = \prod_{i \in I} \varphi^{-1}\left(T_i\right)$$

is a zero-sum subsequence with $|Y| \leq |I| \cdot \max\{|T_i| : 1 \leq i \leq 3n-2\} \leq nm$. To see the sequence is zero-sum, recall $\sigma\left(\varphi^{-1}\left(T\right)\right) = \alpha_i m$, so
$\sigma\left(\prod_{i \in I} \varphi^{-1}\left(T_i\right)\right) = \sum_{i \in I} \alpha_i m = nm \equiv 0 \mod nm$. So the claim is shown. □

While this result is nice, we actually wish to use the result for the s constant. The argument follows the same line of reasoning, with inequalities replaced with equalities.

Theorem 5.3. Let $m, n \in \mathbb{N}$ and suppose it is already known $\mathsf{s}\left(C_m^2\right) = 4m-3$ and $\mathsf{s}\left(C_n^2\right) = 4n-3$. Then $\mathsf{s}\left(C_{mn}^2\right) = 4mn-3$.

Once again, it suffices only to show $4mn-3$ is an upper bound as
$(0,0)^{mn-1}(0,1)^{mn-1}(1,0)^{mn-1}(1,1)^{mn-1}$ is a counterexample of length $4mn-4$.

Proof. The proof follows the same structure. Let $G = C_{mn}^2$ and note
$4mn-3 = m\left(4n-4\right)+4m-3$. Let $\varphi : C_{mn}^2 \to C_m^2, x \mapsto nx$ be the left multiplication by n map. Let $S = \prod_{i=1}^{4mn-3} g_i$ be a sequence in G and let $\varphi\left(S\right) = \prod_{i=1}^{4mn-3} ng_i$. Since $\varphi\left(S\right)$ is a sequence in C_m^2 of length greater than $\mathsf{s}\left(C_m^2\right)$ we find a zero-sum sequence $T_1 \mid \varphi\left(S\right)$ with $|T_1| = m$ so $|\varphi\left(S\right)T^{-1}| = m\left(4n-4\right)+4m-3$. Then, we repeat this process inductively, given a zero-sum subsequence $T_k \mid \varphi\left(S\right)T_1^{-1}\ldots T_{k-1}^{-1}$ with $|T_k| = m$ we find a new zero-sum subsequence $T_{k+1} \mid \varphi\left(S\right)T_1^{-1}\ldots T_k^{-1}$ so that $|T_{k+1}| = m$, so $\left|\varphi\left(S\right)T_1^{-1}\ldots T_{k+1}^{-1}\right| = m\left(4n-3-k-1\right)+4m-3$ for $1 \leq k \leq 4n-5$. At the end we have $4n-4$ disjoint subsequences $T_1, \ldots, T_{4n-4} \mid \varphi\left(S\right)$. Since
$|\varphi\left(S\right)T_1\ldots T_{4n-4}| = 4m-3 = \mathsf{s}\left(C_m^2\right)$, we find one more zero-sum subsequence
$T_{4n-3} \mid \varphi\left(S\right)T_1^{-1}\ldots T_{4n-4}^{-1}$.

Then, noting that each $T_i = \prod_{j=1}^{m} n g_i^{(j)}$ where $g_i^{(j)} \mid S$, $1 \leq j \leq m$ are unique terms in S for each $1 \leq i \leq 4n-3$. Note that $\sigma\left(\varphi^{-1}\left(T_i\right)\right) = \alpha_i m$ for some $\alpha_i \in C_n^2$. So, the sequence

$$X = \alpha_1 \ldots \alpha_{4n-3}$$

is a sequence in C_n^2 with $|X| = \mathsf{s}\left(C_n\right)^2$, so we find $I \subseteq [1, 4n-3]$ so that $|I| = n$ and $|\sigma\left(X\left(I\right)\right)| = 0$. Finally, we see

$$Y = \prod_{i \in I} \varphi^{-1}\left(T_i\right)$$

is a zero-sum subsequence with $|Y| = |I| \cdot m = nm$. To see this sequence is zero-sum recall each $\sigma\left(\varphi^{-1}\left(T_i\right)\right) = \alpha_i m$, so $\sigma\left(\prod_{i \in I} \varphi^{-1}\left(T_i\right)\right) = \sum_{i \in I} \alpha_i m = nm \equiv 0 \mod nm$. So, the claim is shown. □

There is one more theorem in basic zero-sum theory which we will not prove, but is deserving of mention, the davenport constant of an arbitrary rank 2 abelian group.

Theorem 5.4. Let G be a finite abelian group of rank 2, that is $G = C_{n_1} \oplus C_{n_2}$ with $n_1 \mid n_2$. Then, $\mathsf{D}\left(G\right) = \mathsf{D}^*\left(G\right)$.

The proof of this theorem is relatively elementary, following a similar trajectory to theorem 5.2, but it is outside the scope of this thesis so we omit it.

Finally, we now prove the most important result in preparation for our two final theorems, that both η and s are multiplicative. A similar result can be produced for the davenport constant D. Indeed a mirror theorem to theorems 5.2 and 5.3 provides the result. For now, though, we are primarily concerned with the s constant and secondarily concerned with the η constant.

Corollary 5.1. If $\eta\left(C_p^2\right) = 3p-2$ for all primes p, then $\eta\left(C_n^2\right) = 3n-2$ for all $n \in \mathbb{N}$. Similarly, if $\mathsf{s}\left(C_p^2\right) = 4p-3$ for all primes p, then $\mathsf{s}\left(C_n^2\right) = 4n-3$ for all $n \in \mathbb{N}$.

Proof. In either case, $n = \prod_{i=1}^{\ell} p_i^{\alpha_i}$ for some primes p_i and $\alpha_i \in \mathbb{N}$, so applying theorems 5.3 or 5.2 repeatedly will yield the claims. □

With this short introduction to zero-sum theory, we now aim to prove two larger results. The first will show that for all finite abelian p-groups G, we have $\mathsf{D}(G) = \mathsf{D}^*(G)$. The second will show that $\mathsf{s}\left(C_p^2\right) = 4p - 3$ for all $p \in \mathbb{N}$.

Chapter 6

Davenport constant of finite abelian p-groups

Advancing the theme of zero-sum sequences we now aim to determine the davenport constant for finite abelian p-groups. The formal statement is as follows.

Theorem 6.1. Let p be prime, $G = C_{q_1} \oplus C_{q_2} \oplus \ldots \oplus C_{q_d}$ with $q_i = p^{m_i}$ for a prime p and integers $m_i > 0$. Suppose $S = \prod_{i=1}^{\ell} g_i$ is a sequence in G. If $\ell \geq \mathsf{D}^* (G) = 1 + \sum_{i=1}^{d} (q_i - 1)$, then there is a non-empty subset $I \subseteq [1, \ell]$ so that $\sigma (S (I)) = 0$.

The proof of this theorem will once again employ polynomial methods. This time, we do not make use of the Combinatorial Nullstellensatz or any of its variants. Instead, we find polynomials corresponding to which indices get included in I and show that they have sufficiently small degree. Once again, we find it suffices to show that D^* is merely a lower bound of $\mathsf{D} (G)$ as $(1, 0, \ldots, 0)^{q_1 - 1} (0, 1, 0, \ldots, 0)^{q_2 - 1} \ldots (0, 0, \ldots, 1)^{q_d - 1}$ is a sequence of length $\sum_{i=1}^{d} (q_i - 1)$ which necessarily has no zero-sum subsequences.

Map Functors

For the remainder of this proof, F will be a field, $\ell \geq 1$ will be an integer and $\{0, 1\}^{\ell}$ will denote the set of sequences consisting of all 0's and 1's taken from the vector space F^{ℓ}.

Definition 6.1. For a field F and $\ell \geq 0$, define $\mathrm{Map}\left(\{0, 1\}^{\ell}, F\right) = \{f : \{0, 1\}^{\ell} \to F | f \text{ is a function}\}$.

Proposition 6.1. $\mathrm{Map}\left(\{0, 1\}^{\ell}, F\right)$ is an F-vector space with pointwise addition and scalar multiplication. That is, for $f, g \in \mathrm{Map}\left(\{0, 1\}^{\ell}, F\right)$ and $\alpha \in F$ we define $(f + g)(x) = f(x) + g(x)$ and $(\alpha g)(x) = \alpha (g(x))$.

Proof. This statement is routinely checked. First we show the map space to be an abelian

group, then we verify composition produces a F-module and subsequently an F-vector space. Associativity of the map space follows from associativity of F:

$$\begin{aligned}(f+(g+h))(x) &= f(x)+(g+h)(x)\\ &= f(x)+g(x)+h(x)\\ &= (f+g)(x)+h(x)\\ &= ((f+g)(h))(x).\end{aligned}$$

We choose the identity to be the zero map, denoted $\mathbf{0}$.

Additive inverses are satisfied by negation. For $f \in \mathrm{Map}\left(\{0,1\}^{\ell}, F\right)$, we find $-f = -1 \cdot f \in \mathrm{Map}\left(\{0,1\}^{\ell}, F\right)$ and $f + (-f) = \mathbf{0}$.

Finally, commutativity is also inherited from F:

$$(f+g)(x) = f(x)+g(x) = g(x)+f(x) = (g+f)(x).$$

Now, we verify $\mathrm{Map}\left(\{0,1\}^{\ell}, F\right)$ is an F-module. Let $r, s \in F$ and $1 \in F$ to be the multiplicative identity of F. We find, for all $\mathbf{x} \in \{0,1\}^{\ell}$, $(1f)(\mathbf{x}) = 1f(\mathbf{x}) = f(\mathbf{x})$.

Furthermore, left associativity holds :

$$((rs)f)(\mathbf{x}) = (rs)f(\mathbf{x}) = r((sf)(\mathbf{x})) = (r(sf))(\mathbf{x}).$$

Lastly, left distributivity also holds:

$$\begin{aligned}
((r+s)f)(\mathbf{x}) &= (r+s)f(\mathbf{x}) = rf(\mathbf{x}) + sf(\mathbf{x}) \\
&= (rf)(\mathbf{x}) + (sf)(\mathbf{x}) \\
&= (rf+sf)(\mathbf{x}) \\
\text{and } (r(f+g))(\mathbf{x}) &= r((f+g)(\mathbf{x})) \\
&= r(f(\mathbf{x}) + g(\mathbf{x})) \\
&= rf(\mathbf{x}) + rg(\mathbf{x}) \\
&= (rf)(\mathbf{x}) + (rg)(\mathbf{x}) \\
&= (rf+rg)(\mathbf{x})
\end{aligned}$$

.

As these properties hold for composition (multiplication) and the addition operation forms an abelian group, we have thus verifies $\mathrm{Map}\left(\{0,1\}^\ell, F\right)$ is an F-module. Since F is a field, it is then a F-vector space. □

Definition 6.2. For an indexed set $I \subseteq [1,\ell]$ we call a monomial of the form $\prod_{i\in I} x_i$ a **special monomial**.

Proposition 6.2. The set of all special monomials on $F[x_1,\ldots,x_n]$, when interpreted as functions $\{0,1\}^\ell \to F$, forms a basis for $\mathrm{Map}\left(\{0,1\}^\ell, F\right)$.

Proof. Recall $|\mathscr{P}([1,\ell])| = 2^\ell$ where $\mathscr{P}(X)$ denotes the power set of X. Thus, enumerate all possible subsets of $[1,\ell]$ as $J_0, J_1, \ldots, J_{2^\ell-1}$ where $J_0 = \varnothing$, $J_1, \ldots, J_\ell$ are singletons, $J_{\ell+1}, \ldots, J_{\ell+\binom{\ell}{2}}$ are 2-tuples, and so on. In general, $J_{\sum_{i=1}^{k-1}\binom{\ell}{i}+1}, \ldots, J_{\sum_{i=1}^{k}\binom{\ell}{i}}$ are k-tuples for $1 \le k \le \ell$. We see in this way, all J_i are nonempty and ordered by increasing cardinality for $i \in \left[1, 2^l - 1\right]$. Next denote all possible special monomials as

$h_0, h_1, \ldots, h_{2^{\ell-1}} \in F[x_1, \ldots, x_n]$ such that $h_k = \prod_{i \in J_k} x_i$ for each $0 \leq k \leq \ell$. Finally, note that when interpreted as a function, $h_k(x) \in \{0,1\}^\ell$ for $x \in \{0,1\}^\ell$.

First, we must show $\{h_k : 1 \leq k \leq 2^m - 1\}$ is linearly independent. Let $a_i \in F$, $1 \leq i \leq 2^\ell - 1$, so that

$$a_0 h_0 + \sum_{i=1}^{2^\ell - 1} a_i h_i = 0.$$

Noting that $h_0 = \prod_{i \in \varnothing} x_i = 1$ and $h_i(\mathbf{0}) = 0$, $1 \leq i \leq 2^\ell - 1$, we see $a_0 = 0$. Now, let e_n be the vector having 1 in the n'th position and 0 elsewhere. Then, $h_i(\mathbf{e}_n) = 1$ if and only if $h_i = x_n$ or $i = 0$. So, we see

$$0 = \left(\sum_{i=1}^{2^\ell - 1} a_i h_i \right)(e_n) = a_n$$

where $a_n = [x_n] \left(\sum_{i=1}^{2^\ell - 1} a_i h_i \right)$. So, for all $0 \leq i \leq \ell$, we see $a_i = 0$, since these are all the special monomials having at most one variable.

Now, for $n_1, n_2 \leq \ell$ let e_{n_1,n_2} be the vector having 1 in the n_1'th and n_2'th positions and 0 in the others. Similarly to before, we see $h_i(e_{n_1,n_2}) = 1$ if and only if $h_i \in \{x_{n_1}, x_{n_2}, x_{n_1} x_{n_2}\}$. Since $a_{n_1} = a_{n_2} = 0$ (as $n_1, n_2 \leq \ell$) then

$$0 = \left(\sum_{i=1}^{2^\ell - 1} a_i h_i \right)(e_{n_1,n_2}) = a_{n_1,n_2}$$

where once again, $a_{n_1,n_2} = [x_{n_1} x_{n_2}] \left(\sum_{i=1}^{2^\ell - 1} a_i h_i \right)$. So, since there are $\binom{\ell}{2}$ possible monomials with 2 variables, we have $a_i = 0$ for $\ell + 1 \leq i \leq m + \binom{\ell}{2}$. Combining our results yields $a_i = 0$ for $0 \leq i \leq \ell + \binom{\ell}{2}$.

Continuing inductively, assume for all monomials of at most j variables, we find $\left[x_1^{n_1} \ldots x_j^{n_j} \right] = a_{n_1,\ldots,n_j} = 0$. Then, let $e_{n_1,n_2,\ldots,n_{j+1}}$, where $n_1 < n_2 < \ldots < n_{j+1} \leq \ell$, be the vector with 1 in the $n_1, n_2, \ldots, n_{j+1}$ coordinates and 0 elsewhere. Then, applying the previous induction set, we see only the special monomials h_i on $j+1$ variables will have

the property that $h_i\left(e_{n_1,n_2,\ldots,n_{j+1}}\right)=1$ for some $n_1,n_2,\ldots,n_{j+1}$. So,
$0=\left(\sum_{i=1}^{2^\ell-1}a_ih_i\right)\left(e_{n1,n_2,\ldots,n_{j+1}}\right)=a_{n_1,n_2,\ldots,n_{j+1}}$ where
$a_{n_1,\ldots,n_{j+1}}=\left[x_{n_1}x_{n_2}\ldots x_{n_{j+1}}\right]\left(\sum_{i=1}^{2^{m-1}}a_ih_i\right)$. So, $a_k=0$ for all k with
$\sum_{i=1}^{j}\binom{\ell}{i}+1\leq i\leq\sum_{i=1}^{j+1}\binom{\ell}{i}$.

Since $\sum_{i=1}^{\ell}\binom{\ell}{i}=2^\ell-1$, we see this process will terminate after ℓ iterations having proven all $a_i=0$, $0\leq i\leq 2^m-1$. Thus, we see $\{h_i:0\leq i\leq 2^\ell-1\}$ is linearly independent.

Next, we show the set spans $\mathrm{Map}\left(\{0,1\}^\ell,F\right)$. To do this we generalize the prior argument, let e_α be the vector having a 1 in the n'th position if $n\in J_\alpha$ and 0s elsewhere.

Then, we note that $h_\beta\left(e_\alpha\right)=1$ if and only if $J_\beta\subseteq J_\alpha$. Similarly, if e_α is the vector with 1 in the i'th position if $i\in J_\alpha$ and 0's elsewhere, then $h_i\left(e_\alpha\right)=\begin{cases}1, & J_i\subseteq J_\alpha\\ 0, & J_i\not\subseteq J_\alpha\end{cases}$
We use this fact to build a polynomial p which agrees with f for all $\mathbf{x}\in\{0,1\}^\ell$. Note that, by construction, every $\mathbf{x}\in\{0,1\}^\ell$ has a unique $\alpha\in\left[0,2^\ell-1\right]$ so that $e_\alpha=\mathbf{x}$. First, we construct p_0 which agrees with f for all e_α with $|J_\alpha|\leq 0$. This, of course, is simply $p_0\left(\mathbf{x}\right)=f\left(\mathbf{0}\right)h_0\left(\mathbf{x}\right)$. Next, we construct p_1 which agrees with f for all e_α with $|J_\alpha|\leq 1$. This will be $p_1\left(\mathbf{x}\right)=f\left(\mathbf{0}\right)h_0\left(\mathbf{x}\right)+\sum_{\alpha=1}^{\ell}\left(f\left(e_\alpha-f\left(\mathbf{0}\right)\right)h_\alpha\left(\mathbf{x}\right)\right)$. Since $h_i\left(e_\alpha\right)=0$ unless $\alpha=i$, we see $p_1\left(e_\alpha\right)=f\left(\mathbf{0}\right)+\left(f\left(e_\alpha-f\left(\mathbf{0}\right)\right)\right)=f\left(e_\alpha\right)$.

Next, we construct p_2 which will agree with f on all e_α with $|J_\alpha|\leq 2$. For this purpose, let e_{n_1,n_2} be the vector having 1 in the n_1 and n_2 positions and 0 elsewhere, $J_{n_1,n_2}=\{n_1,n_2\}$, and $h_{n_1,n_2}=x_{n_1}x_{n_2}$. Then, the polynomial will be

$$p_2\left(\mathbf{x}\right)=f\left(\mathbf{0}\right)+\sum_{n_1=1}^{\ell}\left(f\left(e_\alpha\right)-f\left(\mathbf{0}\right)\right)h_\alpha\left(\mathbf{x}\right)$$
$$+\sum_{1\leq n_1<n_2\leq\ell}\left(f\left(e_{n_1,n_2}\right)-f\left(e_{n_1}\right)-f\left(e_{n_2}\right)+f\left(\mathbf{0}\right)\right)h_{n_1,n_2}\left(\mathbf{x}\right).$$

It is clear that for all vectors, $\mathbf{x}$, with at most 2 nonzero coordinates, we have $p_2\left(\mathbf{x}\right)=f\left(\mathbf{x}\right)$. We continue on in this manner, inductively construction polynomials over

all sets of size ≤ 3, ≤ 4, and eventually all sets J_α with $|J_\alpha| \leq \ell$. This, of course, covers all the J_α and our polynomial will be:

$$p(\mathbf{x}) \coloneqq p_\ell(\mathbf{x}) = f(\mathbf{0}) h_0(\mathbf{x}) + \sum_{i=1}^{2^\ell - 1} \left(\sum_{j=0}^{|J_i|} \left((-1)^{i-j} \sum_{\substack{J_k \subseteq J_i \\ |J_k| = j}} f(e_k) \right) \right) h_i(\mathbf{x}).$$

This polynomial has the property that $p(\mathbf{x}) = f(\mathbf{x})$ for all $\mathbf{x} \in \{0,1\}^\ell$.

So, $p = f$ and we see $\{h_i : 0 \leq i \leq 2^\ell - 1\}$ spans $\mathrm{Map}\left(\{0,1\}^\ell, F\right)$.

Finally, we conclude $\{h_i : 0 \leq i \leq 2^\ell - 1\}$ forms a basis for the map space. □

Proposition 6.3. Let $f \in \mathbb{Q}[x_1, \ldots, x_\ell]$ be a polynomial taking on integer values when evaluated at $\mathbf{x} \in \{0,1\}^\ell$ and let h_i, $i \in \left[0, 2^\ell - 1\right]$ be all possible special monomials ordered we did previously. Then, there is a $g \in \mathbb{Z}[x_1, \ldots, x_\ell]$ such that $g = \sum_{i \in I} b_i h_i$ for some $I \subseteq \left[0, 2^\ell - 1\right]$ and $b_i \in \mathbb{Z}$ so that, for all $\mathbf{x} \in \{0,1\}^m$, $f(\mathbf{x}) = g(\mathbf{x})$ when evaluated as functions.

Proof. Applying proposition 6.2 yields a g having the desired property that $g(\mathbf{x}) = f(\mathbf{x})$ for $\mathbf{x} \in \{0,1\}^m$ where

$$g(\mathbf{x}) = f(\mathbf{0}) h_0(\mathbf{x}) + \sum_{i=1}^{2^\ell - 1} \left(\sum_{j=0}^{|J_i|} (-1)^{i-j} \sum_{\substack{J_k \subset J_\alpha \\ |J_k| = j}} f(e_k) \right) h_i(\mathbf{x}).$$

Moreover, since $f(\mathbf{0}) \in \mathbb{Z}$ and $\sum_{j=0}^{|J_i|} (-1)^{i-j} \sum_{\substack{J_k \subset J_\alpha \\ |J_k| = j}} f(\mathbf{x}_k) \in \mathbb{Z}$ we see g has integer coefficients. Finally, each h_i is a monomial, so g is the desired sum of monomials. □

Combinatorial Identities

Finally, before we may prove the main theorem, we must show a few binomial identities which we will make use of later.

Proposition 6.4. Let $q = p^m$ for $p \geq 2$ being prime, $m \geq 1$, and $y \in \mathbb{Z}$. Then,

$$\binom{y-1}{q-1} \equiv \begin{cases} 0 \mod p, & y \not\equiv 0 \mod q \\ 1 \mod p, & y \equiv 0 \mod q \end{cases}. \tag{6.1}$$

Additionally, for $n \in \mathbb{Z}$, $\binom{n}{k} \in \mathbb{Z}$

Proof. First, recall

$$\binom{n}{k} = \frac{n\,(n-1)\ldots(n-(k-1))}{k\,(k-1)\ldots(2)\,(1)}.$$

Hence, if $k \leq n$, we find $\binom{n}{k} \in \mathbb{Z}$. Else, if $0 \leq n \leq k-1$, then $\binom{n}{k} = 0 \in \mathbb{Z}$. So, for all $k \in \mathbb{N}$, $n \in \mathbb{Z}$, we have $\binom{n}{k} \in \mathbb{Z}$.

Next, note that

$$\binom{y-1}{q-1} = \frac{(y-1)\,(y-2)\ldots(y-(q-2))\,(y-(q-1))}{(q-1)\,(q-2)\ldots(2)\,(1)}. \tag{6.2}$$

Now, we prove equation (6.1). First, suppose $y \equiv 0 \mod q$, so $y \equiv q \equiv 0 \mod p$, then $y-1 \equiv q-1 \mod p$, $y-2 \equiv q-2 \mod p$ and so on. In general, $y-k \equiv q-k \mod p$ for $1 \leq k \leq q-1$. So, reducing $\mod p$ we find the all factors between the numerator and denominator cancel, yielding $\binom{y-1}{q-1} \equiv 1 \mod p$.

Next, we prove the case $y \not\equiv 0 \mod q$. Note there are $q-1$ factors in the numerator and denominator of equation (6.2). Since $q-1 \equiv p-1 \mod p$, and C_p is cyclic, we find both the numerator and denominator will range over all possible values $k \mod p$, $k \in [0, p-1]$ atleast $\frac{1}{p}\left(p^m - p\right) = p^{m-1} - 1$ times. This, however, only counts $p^m - p$ terms so there must be $p-1$ terms remaining. These terms will once again range over all possible values $k \mod p$ except one. So, in total there is one value $k \mod p$ which is taken on $p^{m-1}-1$ time and all other values $k \mod p$ will be taken on p^{m-1} times. Since we only care about factors of p, we need only check which case the value 0

$\mod p$ falls into. Notice that if $y \not\equiv 0 \mod q$, we find a unique representative $z \in [1, q-1]$ so that $y \equiv z \mod q$. Then, we see $y-1 \equiv z-1 \mod p$, $y-2 \equiv z-2 \mod p, \ldots, y-(q-1) \equiv z-q+1 \equiv z+1 \mod p$, so the value which is taken on only $p^{m-1}-1$ times will be $z \mod p$. Since the denominator has $q-1 \equiv p-1 \mod p, q-2 \equiv p-2 \mod p, \ldots, 1 \equiv 1 \mod p$, we see $0 \mod p$ will be the value which is taken on only $p^{m-1}-1$ times. So, since $z \neq 0$, we have p^{m-1} terms in the numerator which are $0 \mod p$ and only $p^{m-1}-1$ terms in the denominator which are $0 \mod p$. So, after cancelling out like terms, we see $p \mid \binom{y-1}{q-1}$, so $\binom{y-1}{q-1} \equiv 0 \mod p$. □

The Davenport Constant

Now, with the use of all the prior lemmas and propositions, we will state and prove the davenport constant for finite p-groups.

Theorem 6.2 (Davenport Constant of Finite p-group)**.** Let p be prime, $G = C_{q_1} \oplus C_{q_2} \oplus \ldots \oplus C_{q_d}$ with $q_i = p^{m_i}$ for a prime p and integers $m_i > 0$. Suppose $S = \prod_{i=1}^{\ell} g_i$ is a sequence in G. If $\ell \geq \mathsf{D}^*(G) = 1 + \sum_{i=1}^{d}(q_i - 1)$, then there is a non-empty subset $I \subseteq [1, \ell]$ so that $\sigma(S(I)) = 0$.

Proof. To begin, assume indirectly there is a sequence $S = g_1 \ldots g_\ell$ with $\ell \geq \mathsf{D}^*(G)$ and no nontrivial $T \mid S$ with $\sigma(T) = 0$.

Then, we note each $g_i = \left(g_i^{(1)}, g_i^{(2)}, \ldots, g_i^{(d)}\right)$ with each $g_i^{(j)}$ a representative in C_{q_j}, $1 \leq i \leq \ell$. Let $\mathbf{x} = (x_1, \ldots, x_\ell)$ and define $P^* : \{0,1\}^\ell \to \mathbb{Z}$ by $P^*(\mathbf{x}) = \prod_{j=1}^{d} \binom{\left(\sum_{j=1}^{\ell} g_i^{(j)} x_i\right)-1}{q_j - 1}$. Note that we can also interpret P^* as a polynomial in $\mathbb{Q}[x_1, \ldots, x_\ell]$. We will denote this as the polynomial $P \in \mathbb{Q}[x_1, \ldots, x_\ell]$. In general, for a polynomial f, we will denote the function created by evaluating this polynomial as f^*.

By construction, $\sum_{i=1}^{\ell} a_i^{(j)} x_i \in \mathbb{Z}[x_1, \ldots, x_\ell]$ when interpreted as polynomials over $\mathbb{Z}$. Moreover, all such monomials are integer valued on $\{0,1\}^\ell$. Next, we identify each $\mathbf{x} = (x_1, \ldots, x_\ell) \in \{0,1\}^\ell$ with a subsequence $T(\mathbf{x}) \mid S$ where $T(\mathbf{x}) = \prod_{1 \leq i \leq \ell; x_i = 1} g_i$.

Fix $\mathbf{y} \in \{0,1\}^{\ell}$. If $T(\mathbf{x})$ is a nontrivial zero-sum susbequence, then we have $\sum_{i=1}^{\ell} g_i^{(j)} x_i \equiv 0 \mod q_j$ for each $j \in [1,d]$. This is because an element is zero in G, precisely when each of its coordinates is zero in its respective C_{q_i}. So we see proposition 6.3 implies

$$P^*(\mathbf{x}) = \prod_{i=1}^{d} \binom{\left(\sum_{i=1}^{m} g_i^{(j)} x_i\right) - 1}{q_j - 1} \equiv 1 \mod p.$$

On the other hand, if $T(\mathbf{x})$ is not zero-sum, we find a $j_0 \in [1,d]$ so that $\sum_{i=1}^{\ell} g_i^{(j_0)} x_i \not\equiv 0 \mod q_{j_0}$. So, we may applying proposition 6.3 once again to see

$$\binom{\left(\sum_{i=1}^{\ell} g_i^{(j_0)} x_i\right) - 1}{q_j - 1} \equiv 0 \mod p.$$

Thus, $P^*(\mathbf{x}) \equiv 0 \mod p$ as P^* was simply the product over all such binomial coefficients.

So, if $T(\mathbf{x})$ is zero-sum, we have $P^*(\mathbf{x}) \equiv 1 \mod p$, else if $T(\mathbf{x})$ is not zero-sum we find $P^*(\mathbf{x}) \equiv 0 \mod p$. Next, we remark that $\chi_{\mathbf{0}}(\mathbf{x}) = \prod_{i=1}^{\ell} (1 - x_i)$ is the characteristic function for the $\mathbf{0}$ vector.

Then, we see $P^* = \chi_{\mathbf{0}}^* + pQ_1^*$ for some polynomial $Q_1 \in \mathbb{Q}[x_1, \ldots, x_\ell]$. Since P is integer valued on $\{0,1\}^{\ell}$ we can identify it with a polynomial $Q \in \mathbb{Z}[x_1, \ldots, x_\ell]$ by proposition 6.3 such that $P^*(\mathbf{x}) = Q^*(\mathbf{x})$ for all $\mathbf{x} \in \{0,1\}^{\ell}$ where $Q^* : \{0,1\}^{\ell} \to \mathbb{Z}$ is the function induced by Q. Moreover, the proposition guarantees Q is the sum of special monomials.

Now, note that $[x_1 \ldots x_\ell] Q_1(\mathbf{x})$. Then, expanding products, we see $[x_1 \ldots x_\ell](Q(\mathbf{x})) = (-1)^{\ell} + pc_0$. So we see $(-1)^m + pc_0 \not\equiv 0 \mod p$. Thus this coefficient is nonzero. So, since the coefficient of $x_1 \ldots x_\ell$ is nonzero, we find $\deg(Q) \geq \deg(x_1 \ldots x_\ell) = \ell$.

On the other hand, since $x_i \in \{0,1\}$, we note $x_i^k = x_i$ for all $1 \leq i \leq \ell$ and every $k \in \mathbb{Z}$. So, replacing every occurence of x_i^k with x_i, in P, we see we obtain a new polynomial $\widetilde{P}$, with rational coefficients and all terms special monomials which agrees

with P. Since the special monomials form a basis, we see this augmented polynomial has $\widetilde{P} = Q$ as polynomials. Then, since

$$\binom{\left(\sum_{i=1}^{\ell} a_i^{(j)} x_i\right) - 1}{q_j - 1} = \frac{\left(\left(\sum_{i=1}^{\ell} a_i^{(j)} x_i\right) - 1\right) \ldots \left(\left(\sum_{i=1}^{\ell} a_i^{(j)} x_i\right) - (q_j - 1)\right)}{(q_j - 1)!}$$

has each of the $q - 1$ factors of the numerator containing terms of degree at most 1, we see $\deg\left(\binom{\left(\sum_{i=1}^{\ell} a_i(j) x_i\right) - 1}{q_j - 1}\right) \leq q_j - 1$. Thus, $\ell \leq \deg(Q) = \deg\left(\widetilde{P}\right) \leq \sum_{i=1}^{d} (q_i - 1)$ as $\widetilde{P}$ was simply the product over such binomials. So, $\ell \leq \sum_{i=1}^{d} (q_i - 1) < \mathsf{D}^*(G)$, a contradiction by the initial assumptions. Thus, their must in fact be a nontrivial zero-sum subsequence $T(\mathbf{x}) \mid S$, so the claim is shown. □

Remarks

The astute reader may have noticed there are no citations or attributions in this chapter, this is because this proof has gone largely unpublished and without much fanfair. Its arguments mirror that of a paper by Christian Elsholtz in 2007, *Zero-Sum Problems in Finite Abelian Groups and Affine Caps* [5], concerning a similar constant. These methods eventually made their way to David Grynkiewicz, Grynkiewicz and Elsholtz working together at TU Graz, who worked out the details but left the result unpublished. Grynkiewicz, having only reconstructed the arguments, but not writing up all the claims, then gave this proof to a graduate student at the University of Memphis, John Ebert, who would flesh out the proof. Ebert once again left the result unpublished, making this thesis the first time this proof of the upper bound is known to have been published anywhere. While a different proof of the upper bound making use of group rings has been known for quite some time, these more elementary methods provide some insight into how one may approach the general davenport constant problem. Chiefly, the idea to exploit properties and theorems concerning polynomials, perhaps over the product of boolean domains, $\{0, 1\}^m$, corresponding to inclusion of a particular term proves useful in other

applications. Problems naturally arise with this method, namely the lack of commutativity and the p-group structure inherent in our groups, but a general proof may aim to alleviate these problems rather than forge brand new methods.

Chapter 7

The Chevalley-Warning Theorem and Reiher's Proof of the Kemnitz Conjecture

The Chevalley-Warning Theorem

Our first major result of this section concerns the theorem of Chevalley and Warning which gives the conditions under which a certain nontrivial solution to a polynomial in a finite field of characteristic p can exist:

Theorem 7.1 (Chevalley-Warning Theorem [7])**.** Let F be a finite field of characteristic p and let $f_1, f_2, \ldots, f_k \in F[x_1, x_2, \ldots, x_n]$ be polynomials and N the number of points $\mathbf{x} \in F^n$ such that $f_1(\mathbf{x}) = \ldots = f_k(\mathbf{x}) = 0$. If $\sum_{i=1}^{k} \deg(f_i) < n$, then $N \equiv 0 (\text{mod } p)$.

In order to provide a proof of this statement, let us first state and prove the following lemma:

Lemma 7.1 (Lemma)**.** Let F be a finite field and $k_1, k_2, \ldots, k_n \geq 0$ such that

$$\min_{1 \leq i \leq n} k_i \leq |F| - 2.$$

Then, $\sum_{x_1, x_2, \ldots, x_n \in F} x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n} = 0$. (Note: if a 0^0 occurs in the expressions it will be treated as a 1).

Proof. Assume without loss of generality that $k_1 < |F| - 1$. Then, by factoring out a $x_1^{k_1}$ from each term of the sum and grouping all such x_1's, we have $\sum_{x_1, x_2, \ldots, x_n \in F} x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n} = \left(\sum_{x_1 \in F} x_1^{k_1}\right) \sum_{x_2, \ldots, x_n \in F} x_2^{k_2} \ldots x_n^{k_n}$. Hence, we must only show that $\sum_{x_1 \in F} x_1^{k_1} = 0$. Suppose $k_1 = 0$. Then $\sum_{x_1 \in F} x_1^{k_1} = |F|$ and, since p divides $|F|$, we see the case $k_1 = 0$ is trivially true. Now, let $\omega \in F^{\times}$ be a generator of $F^{\times}$. Then,

we have that

$$\sum_{x_1 \in F} x_1^{k_1} = \sum_{x_1 \in F^\times} x_1^{k_1} = \sum_{x_1 \in F^\times} (\omega x_1)^{k_1} = \omega^{k_1} \sum_{x_1 \in F^\times} x_1^{k_1} = \omega^{k_1} \sum_{x_1 \in F} x_1^{k_1}.$$

Taking the difference of the first and last terms of the above equality yields $\left(\omega^{k_1} - 1\right)\left(\sum_{x_1 \in F} x_1^{k_1}\right) = 0$, so either the sum is 0 or $\omega^{k_1} - 1 = 0$. As ω is a generator of the cyclic group $F^\times$, we have $\omega^{k_1} = 1$ only if $k_1 \equiv -1 \pmod{|F|}$. But, as $0 < k_1 < |F| - 1$ this case cannot occur, hence we see $\sum_{x_1 \in F} x_1^{k_1} = 0$, so the lemma is proven. □

Proof of Chevalley-Warning Theorem. First, recall $x^{|F|-1} = x$. Then, define

$$M = \sum_{\mathbf{x} \in F^n} \prod_{i=1}^{k} \left(1 - f_i(\mathbf{x})^{|F|-1}\right).$$

We see, by the earlier proposition, that a term of the sum will be 1 if and only if $\mathbf{x}$ is a solution to the system $f_1, f_2, \ldots, f_k$, else it will be 0. Furthermore, it is clear by the construction that M will be exactly equal to the number of solutions to our system $f_1, \ldots, f_k$, and so $M = N$.

Now, let us define the polynomial $g(\mathbf{x}) = \prod_{i=1}^{k} \left(1 - f_i(\mathbf{x})^{|F|-1}\right)$. Then, repeatedly applying the substitution $x_j^{|F|} \to x_j$ to g yields a polynomial $\overline{g} = g$ for all $\mathbf{x} \in F^n$. Furthermore, $\deg_{x_j}(\overline{g}) \leq |F| - 1$ for $1 \leq j \leq n$ (this is clear as, if it were not we would be able to apply the substitution once again). Then, substituting $\overline{g}$ in place of g yields

$$N = \sum_{\mathbf{x} \in F^n} \overline{g}(\mathbf{x}).$$

Then, applying our lemma, we see that all monomials with degree $|F| - 2$ or less will equal 0 and hence the only possible nonzero terms of $\overline{g}$ are those of the form $\prod_{i=1}^{n} x_i^{|F|-1}$. Expanding the product, we see that such a monomial would be of degree $n(|F| - 1)$, however as $\deg f_i^{|F|-1} = (|F| - 1)\deg(f_i)$, we see that

$\deg(g) \leq (|F|-1)\sum_{i=1}^{k}\deg(f_i) < n(|F|-1)$ by construction. Consequently, any such monomial of $\overline{g}$ (and hence g) will have a zero coefficient, and thus $N \equiv 0 \pmod{p}$. $\square$

Reiher's Proof of the Kemnitz Conjecture

The Chevalley-Warning theorem has found many uses in combinatorics and number theory. One of its most potent results is Christian Reiher's proof of the Kemnitz conjecture [11], one which was produced when Reiher was just and undergraduate. This proof makes heavy use of the Chevalley-Warning Thoerem, as we will see.

Erdos, Ginzburg, and Ziv proved that that $\mathsf{s}(C_n) = 2n-1$. That is, given any sequence of integers of size greater or equal to $2n-1$, we always find a subsequence whose sum is congruent to n. As it turns out $\mathsf{s}(C_n^2)$ is a much more challenging result.

As we have already shown in theorem 5.3, a simple counterxample exist to prove $4n-3$ is a lower bound, so we need only show it is an upper bound. Moreover, corollary 5.1 proves that if the claim holds for n prime, it holds for all n. So, we proceed by showing the claim is true for an arbitrary prime p.

Before we can prove this, however, we must prove several congruencies using theorem 7.1. These lemmas will all require taking three polynomials associated with a given sequence. The first polynomial will ensure sequences of length congruent to p must be taken. The second polynomial will ensure the first coordinates sum to 0, and the third polynomial will ensure the second coordinates sum to 0.

For the remainder of this chapter, $G = C_p^2$ for a prime p.

Lemma 7.2 ([11])**.** Let S be a sequence in G, with $|S| = 3p-3$, then

$$1 - N_{p-1} - N_p + N_{2p-1} + N_{2p} \equiv 0 \mod p.$$

Proof. First, let $\mathbf{F}_p$ be the finite field of characteristic p. Then, denote the terms of S to be (a_i, b_i) for $1 \leq i \leq 3p-3$. Then, define the following three polynomials

$f_1, f_2, f_3 \in F[x_1, \ldots, x_{3p-2}]$ by

$$f_1 = \sum_{i=1}^{|S|} x_n^{p-1} + x_{3p-2}^{p-1}$$
$$f_2 = \sum_{i=1}^{|S|} a_n x_n^{p-1}$$
$$f_3 = \sum_{i=1}^{|S|} b_n x_n^{p-1}.$$

Suppose $\mathbf{x} = (x_1, \ldots, x_{3p-2})$ is a common zero of f_1, f_2, f_3. Then note that $x_i^{p-1} = 1$ if $x_i \neq 0$, so there are two cases. First, if $x_{3p-2} = 0$, we see $f_1(\mathbf{x}) = 0$ implies $\sum_{i=1}^{|S|} x_i^{p-1} \equiv 0 \mod p$, so precisely $0, p$, or $2p$ coordinates $x_i \neq 0$. $\mathbf{x} = \mathbf{0}$ is an obvious common zero. Next, let $I \subseteq [1, 3p-2]$ be the set of indices for the nonzero coordinates, so $x_i \neq 0$ if and only if $i \in I$. Then, we see that $f_1(\mathbf{x}) = \sum_{i \in I} x_i^{p-1} = |I| = 0 \equiv 0 \mod p$, $f_2(\mathbf{x}) \sum_{i \in I} a_i x_i^{p-1} = \sum_{i \in I} a_i \equiv 0 \mod p$, and $f_3(\mathbf{x}) = \sum_{i \in I} b_i x_i^{p-1} = \sum_{i \in I} b_i \equiv 0 \mod p$. So, we need only count over all admissible solutions to f_2, f_3 of size $0, p$, and $2p$ in order to count all possible $\mathbf{x}$ which are common zeroes. The common solutions to f_2, f_3 are simply sequences $S(I) \mid S$ with $\sigma(S(I)) = 0$, so there are N_0, N_p, N_{2p} of them respectively. Moreover, there are $p-1$ possible nonzero $x_i \in C_p$ which can be permuted across the $0, p, 2p$ positions which are nonzero in a common solution. Putting all this together, we obtain $(p-1)^0 N_0 + (p-1)^p N_p + (p-1)^{2p} N_{2p} \equiv 1 - N_p + N_{2p} \mod p$ solutions if $x_{3p-2} = 0$.

Similarly, if $x_{3p-2} \neq 0$, we see there must be $p-1$ or $2p-1$ coordinates nonzero to satisfy f_1. Moreover, letting I be the set of indices which are nonzero (excluding $3p-2$), $f_2(\mathbf{x}) = \sum_{i \in I} a_i \equiv 0 \mod p$ and $f_3(\mathbf{x}) = \sum_{i \in I} b_i \equiv 0 \mod p$ represent zero-sum subsequences of length $p-1$ and $2p-1$ respectively, of which there are N_{p-1} and N_{2p-1} respectively. So permuting over all nonzero $x_i \in C_p$ and all placments of these elements in the, p or $2p$ nonzero indices (now including index $3p-2$) yields $(p-1)^p N_{p-1} + (p-1)^{2p} N_{2p-1} \equiv -N_{p-1} + N_{2p-1} \mod p$ possibilities.

Totaling the cumulative number of solutions, we find

$$1 - N_{p-1} - N_p + N_{2p-1} + N_{2p}$$

solutions to $f_1 = f_2 = f_3 = 0$. Since we have 3 polynomials over $3p - 2 \geq 4$ variables, with $\deg(f_1) + \deg(f_2) + \deg(f_3) = 3(p-1) < 3p - 2$ we find the number of solutions congruent to $0 \mod p$ by applying theorem 7.1. □

The following lemma all follow from essentially the same argument using the given set of polynomials:

Lemma 7.3 ([11])**.**

If $|S| = 3p - 2$ or $|S| = 3p - 1$, then

$$1 - N_p + N_{2p} \equiv 0 \mod p. \tag{7.1}$$

Moreover, $N_p \equiv 0$ implies $N_{2p} \equiv -1$.

Proof. The second assertion follows directly from the first, so we need only show equation (7.1). Again, we define the following polynomials

$$f_1 = \sum_{i=1}^{|S|} x_n^{p-1}$$
$$f_2 = \sum_{i=1}^{|S|} a_n x_n^{p-1}$$
$$f_3 = \sum_{i=1}^{|S|} b_n x_n^{p-1}.$$

Since we have no excess variable like in the last proof, we apply the same arguments as the first case of the previous lemma. Let $\mathbf{x} = (x_1, \ldots, x_{3p-2})$ be a common zero of

f_1, f_2, f_3. $f_1(\mathbf{x}) = 0$ requires the number of $x_i \neq 0$ to be congruent to $0 \mod p$, so a possible common zero must have $0, p, 2p$ nonzero coordinates. Next, $f_2(\mathbf{x}) = f_3(\mathbf{x}) = 0$ requires the subsequence $T(\mathbf{x})$ induced by the nonzero x_i to be zero-sum. All together, for the case of 0 nonzero coordinates we find one possibility, for the case of p nonzero coordinates we find $(p-1)^p N_p$ possibilities and for the case of $2p$ nonzero coordinates we find $(p-1)^{2p} N_{2p}$ possibilities. Summing, we find $1 - N_p + N_{2p}$ possible solutions. Since $\deg(f_1) + \deg(f_2) + \deg(f_3) = 3p - 3 < 3p - 2$ we can apply theorem 7.1 to see $1 - N_p + N_{2p} \equiv 0 \mod p$. Applying the same methods as lemma 7.2 yields

$$1 + (p-1)^p N_p + (p-1)^{2p} N_{2p}$$

solutions. Evaluating the coefficients and applying Chevalley-Warning yields the result. □

Lemma 7.4 ([11])**.** If $|S| = 4p - 3$, then

$$-1 + N_p - N_{2p} + N_{3p} \equiv 0 \mod p \text{ and,} \tag{7.2}$$

$$N_{p-1} - N_{2p-1} + N_{3p-1} \equiv 0 \tag{7.3}$$

Proof. This is proved analogously to the previous lemmas. First, we show (7.2) by taking the following polynomials

$$f_1 = \sum_{i=1}^{|S|} x_n^{p-1}$$
$$f_2 = \sum_{i=1}^{|S|} a_n x_n^{p-1}$$
$$f_3 = \sum_{i=1}^{|S|} b_n x_n^{p-1}.$$

Applying the same argument as the previous lemmas yields

$$1 + (p-1)^p N_p + (p-1)^{2p} N_{2p} + (p-1)^p N_{3p}$$

solutions. Evaluating the coefficients and applying Chevalley-Warning yields

$$1 - N_p + N_{2p} - N_{3p} \equiv 0 \mod p.$$

Finally, negating this yields result (7.2).

Similarly, for (7.3) we use the polynomials

$$\begin{aligned} f_1 &= \sum_{i=1}^{|S|} x_n^{p-1} + x_{4p-2}^{p-1} \\ f_2 &= \sum_{i=1}^{|S|} a_n x_n^{p-1} \\ f_3 &= \sum_{i=1}^{|S|} b_n x_n^{p-1}. \end{aligned}$$

Counting solutions yields

$$\begin{aligned} &1 + (p-1)^p N_p + (p-1)^{2p} N_{2p} + (p-1)^{3p} N_{3p} \\ &\quad + (p-1)^p N_{p-1} + (p-1)^{2p} N_{2p-1} + (p-1)^{3p} N_{3p-1} \end{aligned}$$

solutions. Evaluating coefficients and applying Chevalley-Warning theorem yields

$$1 - N_p + N_{2p} - N_{3p} - N_{p-1} + N_{2p-1} - N_{3p-1} \equiv 0.$$

As we already know the first 4 terms to be congruent to 0 negating what is left yields equation (7.3) □

These lemmas make full use of the Chevalley-Warning theorem and show its power in

proving these sorts of combinatorial results. Before we can present the proof of the main theorem (the Kemnitz conjecture) we need to prove a few more lemmas.

Lemma 7.5 ([11])**.** If $|S| = 4p - 3$, then

$$3 - 2N_{p-1} - 2N_p + N_{2p-1} + N_{2p} \equiv 0 \mod p. \tag{7.4}$$

Proof. Denoting $\mathscr{I}$ to be the set of all subsequences $I \mid S$ with $|I| = 3p - 3$, we can apply 7.2 to each $I \in \mathscr{I}$ to see

$$\sum_{I \in \mathscr{I}} \left[1 - N_{p-1}(I) - N_p(I) + N_{2p-1}(I) + N_{2p}(I)\right] \equiv 0. \tag{7.5}$$

We find there are $\binom{4p-3}{3p-3}$ possible sets I. Then, for a given zero sum subsequence of length $p-1$ in X, we see we can form a set $I \subseteq \mathscr{I}$ by simply appending $2p-2$ elements to the subsequence. We find there are $\binom{3p-2}{2p-2}$ possibilities for these appendices to form I. Similarly, given a zero sum subsequence of length p we find $\binom{3p-3}{2p-3}$ possible sets I containing the sequence. For a sequence of length $2p-1$ we find $\binom{2p-2}{p-2}$ possibilities and for a sequence of length $2p$, we find $\binom{2p-3}{p-3}$ possibilities.

Permuting over all such zero-sum sequences in J yields

$$\begin{aligned}\text{Equation (7.5)} = \binom{4p-3}{3p-3} - \binom{3p-2}{2p-2}N_{p-1} - \binom{3p-3}{2p-3}N_p \\ + \binom{2p-2}{p-2}N_{2p-1} + \binom{2p-3}{p-3}N_{2p} \equiv 0 \mod p.\end{aligned}$$

Finally, expanding and reducing the binomial coefficients modulo p much as in proposition 6.4 yields equation (7.4). □

Before we may prove the main result we need just a few more lemmas:

Lemma 7.6 ([2])**.** Let S be a sequence in G and suppose there is a zero-sum subsequence $T \mid S$ with $|T| = 3p$. Then, $N_p(S) > 0$

Proof. Let $t \mid T$, since $|Tt^{-1}| = 3p - 1$, we may apply lemma 7.3 to see $N_p(Tt^{-1}) \equiv 0 \mod p$ implies $N_{2p}(Tt^{-1}) \equiv -1 \mod p$. Assume $N_p(Tt^{-1}) = 0$, then since $N_{2p}(Tt^{-1}) \neq 0$, we find a zero-sum subsequence $T_1 \mid Tt^{-1}$with $|T_1| = 2p$. But then, $\sigma(T) = \sigma(T_1) + \sigma\left(TT_1^{-1}\right)$, so $\sigma\left(TT_1^{-1}\right) = 0$. Since $\left|TT_1^{-1}\right| = p$ this is a contradiction, so $N_p(Tt^{-1}) \neq 0$ and since any zero-sum subsequence in Tt^{-1} is also a subsequence in S, we see $N_p(S) > 0$. □

We prove one final lemma:

Lemma 7.7 ([11])**.** If $|S| = 4p - 3$ and $N_p = 0$, then $N_{p-1} \equiv N_{3p-1} \mod p$. Consequently,

$$N_{p-1} - N_{3p-1} \equiv 0 \mod p. \tag{7.6}$$

Proof. Let N denote the number of partitions of S into 3 disjoint subsequences, A, B, C with

$$|A| = p - 1, |B| = p - 2, \text{ and } |C| = 2p \tag{7.7}$$

so that

$$\sigma(A) = \sigma(C) \equiv 0 \mod p \text{ and consequently } \sigma(B) \equiv \sigma(X) \mod p. \tag{7.8}$$

First, we note that

$$N \equiv \sum_A N_{2p}\left(SA^{-1}\right)$$

where $\sum_A$ denotes the sum over all sets $A \subseteq X$ so that (7.7) and (7.8) hold. Note that this simply counts the number of admissible C for each possible set A, leaving whatever points remain to belong to B, thereby counting the number of possible partitions (modulo

p). Next, since $|SA^{-1}| = 3p-2$, we may apply 7.3 to see $N \equiv \sum_A -1 \equiv -N_{p-1}(S) \mod p$.

Applying the same method, but over B, we see $N \equiv \sum_B N_{2p}(SB^{-1})$, by counting all possible sets C for each admissible B. As $|SB^{-1}| = 3p-1$, we may once again apply 7.3 to find $N \equiv \sum_{X-B} -1 \equiv -N_{3p-1} \mod p$.

By method of double counting we attain $N_{p-1} \equiv N_{3p-1}$, the desired result. □

With many small parts proven, we need simply combine them to yield the Kemnitz conjecture.

Theorem 7.2.

$$\mathsf{s}\left(C_n^2\right) = 4n-3.$$

Proof of the Kemnitz Conjecture [11]. Adding the equations we have obtained thus far, we see for $|S| = 4p-3$ we have

$$\begin{aligned}
&(7.2)+(7.3)+(7.4)+(7.6) \text{ yields} \\
&-1+N_p-N_{2p}+N_{3p}+N_{p-1}-N_{2p-1}+N_{3p-1}+3-2N_{p-1} \\
&\quad -2N_p+N_{2p-1}+N_{2p}+N_{p-1}-N_{3p-1} \\
&\quad = 2-N_p+N_{3p} \equiv 0 \mod p
\end{aligned}$$

If p is an odd prime, we see the statement $N_p \equiv N_{3p} \equiv 0 \mod p$ cannot be true (as $2 \not\equiv 0$), Hence, either $N_p \not\equiv 0$ in which case the claim is shown, or $N_{3p} \not\equiv 0$ implying S contains a subsequence of size $3p$ whose sum is zero. Applying lemma 7.6 then yields that $N_p > 0$, so the claim is shown in this case as well. Else, if $p = 2$ note that if a sequence contains any repeated element, it has a zero-sum subsequence of length 2 (taking both copies of the repeated element). Since $|C_2^2| = 4$, any sequence of $5 = 4 \cdot 2 - 3$ elements will contain a repeated element, and thus a zero-sum subsequence of length 2, so this case

holds as well. Since the claim holds for all primes p, we see corollary 5.1 implies $C_n^2 = 4n - 3$, so the Kemnitz conjecture it true. $\square$

Chapter 8

Conclusion

Ultimately, the polynomial method proves quite useful. It's many variations are able to solve problems from number theory, combinatorics, zero-sum theory, graph theory, and many other domains. While we only touched on some of the basic tools and methods in this Thesis, many of these ideas can be expanded further to prove even stronger results. For example, there are generalized Chevalley-Warning theorems. Other ideas prove harder to generalize. For instance, determining the value of $\mathsf{s}\left(C_n^3\right)$ is still an open problem, as is $\mathsf{D}\left(G\right)$ for an arbitrary abelian group G. In these cases existing polynomial methods fall short. In the end, though, the breadth and complexity of the problems that can be solved with polynomial methods is quite remarkable and deserving of further study. We hope the general reader has picked up at least some ideas concerning polynomials and their usefulness which they can introduce into their mathematical toolkit.

REFERENCES

[1] Noga Alon. Combinatorial nullstellensatz. *Combinatorics, Probability and Computing*, 8(1-2):7–29, 1999.

[2] Noga Alon and Moshe Dubiner. A lattice point problem and additive number theory. *Combinatorica*, 15:301–309, 1995.

[3] Noga Alon, Melvyn B. Nathanson, and Imre Ruzsa. The polynomial method and restricted sums of congruence classes. *Journal of Number Theory*, 56(2):404–417, February 1996.

[4] George Andrews. Proc. advanced sem., math. res. center, univ. wisconsin, madison, wis., 1975. In Richard Askey, editor, *Problems and Prospects for Basic Hypergeometric Functions*, pages 191–224. Academic Press, Math Res. Center, Univ. Wisconsin, 1975.

[5] Yves Edel, Christian Elsholtz, Alfred Geroldinger, Silke Kubertin, and Laurence Rackham. Zero-Sum Problems in Finite Abelian Groups and Affine Caps. *The Quarterly Journal of Mathematics*, 58(2):159–186, 05 2007.

[6] I. J. Good. Short proof of a conjecture by dyson. *Journal of Mathematical Physics*, 11(6):1884–1884, 1970.

[7] David J. Grynkiewicz. *Structural additive theory*, chapter The Polynomial Method: The Erdos:Heilbronn Conjecture. Springer, 2013.

[8] Gyula Károlyi and Zoltán Nagy. A simple proof of the zeilberger–bressoud q-dyson theorem. *Proceedings of the American Mathematical Society*, 142(9):3007–3011, Sep 2014.

[9] Madan Lal Mehta and Freeman J. Dyson. Statistical theory of the energy levels of complex systems. v. *Journal of Mathematical Physics*, 4(5):713–719, 1963.

[10] D. Nelson. *The Penguin Dictionary of Mathematics*. Penguin reference library. Penguin Books Limited, 4 edition, 2008.

[11] Christian Reiher. On kemnitz' conjecture concerning lattice-points in the plane. *The Ramanujan Journal*, 13, Jun 2007.

[12] Thomas Sauer and Yuan Xu. On multivariate lagrange interpolation. *Mathematics of Computation*, 64(211):1147–1170, 1995.

[13] B.L. Van der Waerden. *Modern Algebra*. Julius Springer, 1931.

[14] Kenneth G. Wilson. Proof of a conjecture by dyson. *Journal of Mathematical Physics*, 3(5):1040–1043, 1962.